PAN-OS® 7.1 Release Notes

Release 7.1.10

Revision Date: May 22, 2017

Review important information about Palo Alto Networks PAN-OS 7.1 software, including new features introduced, workarounds for open issues, and issues that are addressed in the PAN-OS 7.1 release. For installation, upgrade, and downgrade instructions, refer to the PAN-OS 7.1 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 7.1 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 7.1

The following topics describe the new features introduced in PAN-OS® 7.1 releases, which require content release version 564 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 7.1 New Features Guide. The new features guide also provides additional information about how to use the new features in this release.

Management Features

New Management Feature	Description
Commit Queues	The firewall and Panorama™ now queue commit operations so that you can initiate a new commit while a previous commit is still in progress. This enables you to activate configuration changes without having to coordinate commit times with other administrators. For example, after reconfiguring a firewall locally, you can initiate a firewall commit while it is still receiving device group and template settings that a Panorama administrator committed. In Panorama, you can also initiate a single commit to push settings from multiple device groups that target different virtual systems on the same firewall instead of committing from one device group at a time.
Synchronization of SNMP Trap and MIB Information	When an event triggers SNMP trap generation (for example, an interface goes down), the firewall, Panorama virtual appliance, M-Series appliance, and WF-500 appliance now update the corresponding SNMP object in response (for example, the interfaces MIB) instead of waiting for the 10-second timer to expire and allowing SNMP queries to receive out-of-sync replies. This ensures that your network management system displays the latest information when polling an object to confirm the event.
Banners and Message of the Day	For the firewall and Panorama, you can now customize the web interface as follows: • Force administrators to acknowledge the login banner to ensure they see information they need to know before they log in, such as login instructions. • Add a *message of the day* that displays in a dialog after administrators log in to ensure they see important information, such as an impending system restart, that can affect their tasks. The same dialog also displays messages that Palo Alto Networks embeds to highlight important information associated with a software or content release. • Add colored bands that highlight overlaid text across the top (*header banner*) and bottom (*footer banner*) of the web interface to ensure administrators see critical information, such as the classification level for firewall administration.
Support for Certificates Generated with 4,096-bit RSA Keys	The firewall and Panorama now support certificates generated with 4,096-bit RSA keys, which are more secure than smaller keys. You can use these certificates to authenticate clients, servers, users, and devices in several applications, including SSL/TLS decryption, Captive Portal, GlobalProtect™, site-to-site IPSec VPN, and web interface access.
Bootstrapping Firewalls for Rapid Deployment	For agility and efficiency in deploying the Palo Alto Networks next-generation firewall at a remote site or at a data center, you can now fully provision (*bootstrap*) a firewall with or without Internet access. Bootstrapping reduces operational effort and service-ready time by eliminating manual configuration steps and user errors when deploying new firewalls. You can now bootstrap the firewall using an external device—a USB flash drive or a virtual CD ROM/DVD—and accelerate the process of configuring and licensing the firewall. The bootstrapping process is supported on all hardware-based firewalls and on VM-Series firewalls in both the private cloud (KVM, ESXi, Hyper-V) and the public cloud (AWS, Azure). Starting with PAN-OS 7.1.4, you can bootstrap the KVM edition of the VM-Series firewall in an OpenStack environment.
Web Interface Design Refresh	The web interface design on Panorama and the firewalls is redesigned with new icons and buttons and an updated font and color scheme. This modernization does not include any changes in layout or workflows to ensure that you do not need to re-familiarize yourself with the user interface.

New Management Feature	Description
New API Request to Show PAN-OS Version	You can now use the PAN-OS XML API to show the PAN-OS version on a firewall or Panorama. In addition to the PAN-OS version, this new API request type (`type=version`) provides a direct way to obtain the serial number and model number.
Unified Logs	A new unified log view allows you to view the latest Traffic, Threat, URL Filtering, WildFire™ Submissions, and Data Filtering logs on a single page. While the individual log views are still available for these log types, the unified log view enables you to investigate and filter these different types of logs in a single view. 💡 Unified logs also allows you to perform a search from AutoFocus to a targeted firewall or Panorama. Learn more about how to use AutoFocus with a firewall or Panorama.
AutoFocus and PAN-OS Integrated Logs	AutoFocus™ threat intelligence data is now integrated with PAN-OS logs, providing you with a global context for individual event logs. You can now click on an IP address, URL, user agent, filename, or hash in a PAN-OS log entry to display an AutoFocus threat intelligence summary of the latest findings and statistics for that artifact. Use the new AutoFocus summary for log entry artifacts to quickly assess the pervasiveness and risk of an artifact while still in the firewall or Panorama context. You can then open an expanded AutoFocus search directly from the firewall or Panorama. 💡 Explore the features that allow you use AutoFocus with a firewall or Panorama.
Administrator Login Activity Indicators	To detect misuse and prevent exploitation of administrator accounts on a Palo Alto Networks firewall or Panorama, the web interface and the command line interface (CLI) now display the last login time and any failed login attempts when an administrator logs in to the interface. These administrator login activity indicators allow you to easily identify whether someone is using your administrative credentials to launch an attack.

App-ID Features

New App-ID™ Feature	Description
PDF Report for Visibility into SaaS Applications	The new SaaS application usage PDF report provides visibility into the SaaS applications in use on your network. SaaS is a way of delivering applications where the service provider owns and manages the software and the infrastructure, and the user controls the data, including the rights to who can create, access, share, and transfer data. The new report helps you identify the ratio of sanctioned versus unsanctioned SaaS applications in use on the network and includes details on the top SaaS application subcategories by number of applications, by number of users, and by volume of data transferred using these applications. The key findings in this report summarize how your SaaS application usage compares to most Palo Alto Networks customers and the percentage of your users who use one or more unsanctioned SaaS applications. You can use the data from this report to define or refine security policy rules on the firewall to block or monitor the use of unsanctioned SaaS applications on your network.

Virtualization Features

New Virtualization Feature	Description
VM-Series Firewall for Microsoft Azure	The VM-Series firewall can now be deployed in Azure, the Microsoft public cloud. The VM-Series firewall can be deployed as a gateway that secures and integrates your multi-tier applications and services in the Azure cloud and the corporate office or enterprise data center, and as a next-generation firewall that secures inter-application traffic within the Azure cloud. VM-Series firewall options through the Azure Marketplace include the bring your own license (BYOL) model and two options (Bundle 1 and Bundle 2) for the hourly pay-as-you-go (PAYG) model. PAN-OS 7.1.1 adds support for the VM-Series on Azure Government, which is a public cloud platform for U.S. government and public sector agencies. On the Azure Government Marketplace, the VM-Series firewall is only available as a bring your own license (BYOL) option because the Azure Government Marketplace does not support pay-as-you-go (PAYG).
Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall	When using the VM-Series NSX edition solution for automated provisioning of VM-Series firewalls, you can now create multiple service definitions on Panorama. You can now have separate Security policy rules for VM-Series firewalls deployed on different ESXi clusters but managed by a vCenter Server and NSX Manager. This capability allows you to define tenant-specific Security policy rules for securing guest virtual machines within an ESXi cluster. Each service definition (up to 32 are supported) includes a template, a device group, and the license auth codes for firewalls deployed using this service definition. Additionally, you can configure Access Domains on Panorama to limit administrative access to a specified set of firewalls. The VM-Series firewall now also supports multiple zones and virtual wire interface pairs, allowing you to create zone-based policy rules with a single (common) set of Security policy rules for guest virtual machines that belong to different tenants or departments; traffic separation is made possible by allocating a unique zone and pair of virtual wire interfaces for guest virtual machines that belong to a specific tenant or department. This capability also allows you to enforce policy on guest virtual machines that have overlapping IP addresses, typically seen in cases where the guest virtual machines are assigned to separate VLANs, VXLANs, or Security groups in the vSphere environment.
VM-Series Firewall for Microsoft Hyper-V	To expand support for deploying the VM-Series firewall in private cloud and hybrid cloud environments, you can now deploy the VM-Series firewall on Hyper-V Server 2012 R2 (standalone edition) or Windows Server 2012 R2 (standard and datacenter editions) with the Hyper-V role that lets you create and manage virtual machines. You can deploy one or more instances of the VM-Series firewall using the Hyper-V Manager (guided user interface) or Windows PowerShell (command line interface). Tap, virtual wire, Layer 2, and Layer 3 interface modes are supported.
Support for VMware Tools on Panorama and on VM-Series Firewalls on ESXi	For ease of administration, the VM-Series firewall and the Panorama virtual appliance are now bundled with a customized version of open-vm-tools. This bundle allows the virtual infrastructure administrator to: • View the management IP address and PAN-OS version of the firewall and Panorama on vCenter. • View resource utilization metrics for the hard disk, memory, and CPU. • Monitor availability and health status of the virtual appliance using a heartbeat mechanism. • Gracefully shutdown and restart the firewall and Panorama from the vCenter server.

New Virtualization Feature	Description
Support for Device Group Hierarchy in the VM-Series NSX Edition Firewall	With this enhancement, you can now assign the VM-Series NSX edition firewall to a template stack and a device group in a hierarchy so that the firewalls can inherit settings defined in the stack and the hierarchy. As you provision or power off virtual machines in the vSphere environment, you can enable notification of IP address changes to one or more device groups in a hierarchy. This notification allows Security policy rules that reference Dynamic Address Groups to collect information on the changes and dynamically drive policy updates to secure the network.
Support for Synchronizing VM Monitoring Information on Firewalls in HA	For a pair of firewalls (VM-Series and hardware-based firewalls) deployed in a high availability configuration, dynamic data such as information about virtual machine IP addresses and other monitored attributes, can now be synchronized between HA peers.
Support for Amazon ELB on the VM-Series Firewalls in AWS	To use Amazon Elastic Load Balancing (ELB) for increased fault tolerance in your AWS deployment, you can deploy the VM-Series firewall behind the Amazon ELB. Each instance of the VM-Series firewall can send traffic to one EC2 instance. To integrate with the Amazon ELB, you must swap the management interface (eth0) and dataplane interface (eth1) on the VM-Series firewall so that the primary interface (management) on the VM-Series firewall can receive dataplane traffic. A new CLI command (`set system setting mgmt-interface-swap enable yes`) allows you to swap the management interface (eth0) and dataplane interface (eth1) so that the firewall can send and receive dataplane traffic on eth0. With this change, the Amazon ELB can automatically monitor the health of the VM-Series firewalls and route traffic to healthy instances of the VM-Series firewall in the same or across Availability Zones.
VM-Series License Deactivation API Key	In PAN-OS 7.1.7 and later PAN-OS 7.1 releases, to deactivate a VM-Series license you must first install a license API key on your firewall or Panorama. The deactivation API key provides an additional layer of security for communications between the Palo Alto Networks Update Server and VM-Series firewalls and Panorama. The PAN-OS software uses this API key to authenticate with the update and licensing servers. The API key is available through the Customer Support Portal to administrators with superuser privileges.

WildFire Features

New WildFire Features	Description
Five Minute WildFire Updates	The WildFire public cloud now globally distributes virus and DNS signatures every five minutes to Palo Alto Networks firewalls. This quick distribution enables firewalls with a WildFire subscription to detect and block threats within minutes of discovery. With earlier PAN-OS release versions, WildFire updates are made available every fifteen minutes.
Mac OS X File Analysis	A Palo Alto Networks firewall can now automatically forward Mac OS X files for WildFire analysis. The minimum content release version required to support this feature is 582.
New WildFire API Features	You can now use the WildFire API on the WildFire public cloud and WF-500 appliance to submit links for WildFire analysis and to get verdicts for samples.

Content Inspection Features

New Content Inspection Features	Description
Enhanced Security for Application and URL Category-Based Policy New in PAN-OS 7.1.1	A new security enhancement prevents evasions of policy rules that block or allow traffic based on URL category and/or application. Now, after a firewall performs DNS resolutions to classify traffic as belonging to an App-ID or a URL category, the firewall also checks to ensure that the hostname or SNI indicated in the initial HTTP or TLS request corresponds to the destination IP address for the established session. To benefit from the increased security for application and URL category-based policy rules, you must: □ Upgrade the firewall to PAN-OS 7.1.1. □ Install the Applications and Threats content version 579 or a later release. □ Set up the firewall to act as a DNS proxy—this allows the firewall to ensure that DNS resolutions match connecting clients. □ Configure an anti-spyware profile to alert on or block traffic that matches the signatures 14984 and 14978, and attach the anti-spyware profile to a policy rule. Review this detailed workflow to make sure you have enabled prevention for HTTP hostname and TLS SNI evasions.
Protection Against LZMA Compressed Adobe Flash Files	The firewall now supports hash-based protection against malicious Adobe flash files that have undergone Lempel-Ziv-Markov chain algorithm (LZMA) compression. Though LZMA compression is a legitimate type of compression that allows data to be reconstructed in its original form without data loss, it can also be used to compress malicious files so that they evade detection.
Extended Support for URLs and Domain Names in an External Dynamic List	External Dynamic Lists (formerly called Dynamic Block Lists) now support URLs and domain names in addition to IP addresses. External dynamic lists allow you to automate and simplify the process of importing URLs, domain names, and IP addresses into the firewall. These lists allow you to take prompt action when you receive threat intelligence from external sources because they do not require a configuration change or commit on the firewall. For domains, you can configure the firewall to alert, block, or sinkhole traffic when performing a DNS resolution. For URLs, you can trigger an alert or block the traffic when the user makes an HTTP request. IP address lists continue to be available for use in policy rules and are best suited for enforcing an IP block list. Each External Dynamic List can include entries of one type only—IP address, URL, or domain. You cannot combine different types of entries in a single list.
TCP Sessions and Content-ID™ Settings in the Web Interface.	Now, all of the settings required to protect your network from Layer 4 and Layer 7 evasions are available in the web interface for simplified configuration. These settings were previously only available from the CLI.

GlobalProtect Features

New GlobalProtect Feature	Description
GlobalProtect App for Chrome OS	The new GlobalProtect app for Chrome OS is now available for Chromebooks running Chrome OS 45 and later. The app, which is available from the Chrome Web Store, extends the same next-generation firewall-based policies that are enforced within the physical perimeter to devices running Chrome OS. GlobalProtect portals and gateways support the GlobalProtect app for Chromebooks in PAN-OS 6.1 and later releases.
Simplified GlobalProtect Agent User Interface for Windows and Mac OS Clients	The GlobalProtect agent 3.0 for Windows and Mac OS now displays a simpler, cleaner user interface. As part of the redesign, a user can now log in to the GlobalProtect portal and view connection status information right from the main **Home** tab. The remaining tabs provide details and statistics about the connection, information that the GlobalProtect agent is collecting about the host state, and troubleshooting information.
Dynamic GlobalProtect App Customization	New configuration options for the GlobalProtect app will now be available with content releases. This change will allow you to take advantage of new app configuration features without waiting for the next PAN-OS release. With this feature, you can also view all customization options from the new **App** tab in a GlobalProtect portal agent configuration. Configure these options to change the default display of the GlobalProtect user interface, usability preferences, timeout values, and scenario-based behaviors. Included in the new customization options are settings that, in earlier releases, required you to define their values in the Windows registry or Mac global property list (plist). Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows registry or the Mac plist.
Enhanced Two-Factor Authentication for GlobalProtect	Two-factor authentication is now easier to deploy and use. By pre-deploying a client certificate through the Simple Certificate Enrollment Protocol (SCEP) and by enabling dynamic passwords, such as one-time passwords (OTPs), you make strong two-factor authentication easier, as follows: • Client certificate distribution—For easier deployment, the GlobalProtect portal can now request a client certificate from your enterprise public key infrastructure (PKI) and issue the certificate to a user—without exposing the PKI infrastructure to the Internet. The client certificate has a configurable lifespan, typically 90 days. GlobalProtect automates the process by using SCEP to obtain and install certificates transparently, thus simplifying the deployment of credentials. • Cookie authentication—To reduce the number of times users must enter their two-factor authentication credentials, you can now configure GlobalProtect to require users to log in only once when connecting to GlobalProtect portals and gateways. After a user authenticates and connects, GlobalProtect creates an encrypted cookie and issues it to the GlobalProtect agent. With an encrypted cookie on their device, users can remain logged in for the lifespan of the cookie (typically 24 hours). For each subsequent login during the lifespan of the cookie (for example, after the device wakes up from the sleep state), GlobalProtect uses the cookie to authenticate the user instead of requiring the user to enter credentials. The new authentication override options replace the authentication modifier option, which was available in PAN-OS 7.0. For upgrade information on this feature, see Upgrade/Downgrade Considerations.

New GlobalProtect Feature	Description
Client Authentication Configuration by Operating System or Browser	For increased flexibility, you can now specify the client operating system (Android, iOS, Windows, Mac, or Chrome), to which to apply a client authentication configuration. You can also customize the client authentication for satellite devices, web-based browser access (GlobalProtect portal only), and third-party IPSec VPN access (GlobalProtect gateways only). This enhancement enables you to customize the authentication method for different sets of users.
Kerberos Single Sign-On for GlobalProtect	GlobalProtect clients running on Windows 7, 8, or 10 now support Kerberos V5 single sign-on (SSO) for GlobalProtect portal and gateway authentication. In this implementation, the GlobalProtect portal and gateway act as Kerberos service principals, and the GlobalProtect app acts as a user principal and authenticates the user with a Kerberos service ticket from the Key Distribution Center (KDC). Kerberos SSO is primarily intended for internal gateway configurations to provide accurate User-ID™ information transparently without any user interaction.
Customizable Password Expiry Notification Message	You can now customize the notification message that GlobalProtect displays when a user's password is about to expire. The new option is available in the GlobalProtect portal agent configuration and is supported using the LDAP authentication method. The GlobalProtect agent appends the custom message to the standard password expiry notification message that it displays before a user's password expires. This enhancement enables you to display information that users may need when their password is about to expire.
Enhanced Authentication Challenge Support for Android and iOS Devices	GlobalProtect for iOS and Android devices now supports two-factor authentication challenge as a one-time password (OTP). When prompted, the user can now cancel the login to view the token password sent via SMS or using any other token retrieval app on the mobile device. The user must then return to the GlobalProtect app and log in with the valid token password within 30 seconds. If the user does not successfully enter the password within 30 seconds, the authentication challenge disappears and the user must restart the GlobalProtect app to enter the password.
Block Access from Lost or Stolen and Unknown Devices	For greater protection against unauthorized network access, you can now block access from known and unknown devices. To block network access from known devices, you can now add host IDs to a device block list. This is useful when a user reports that a device is lost or stolen and you need to take immediate action. To prevent unauthorized access from unknown devices, you can now configure the firewall to pre-deploy client certificates through the Simple Certificate Enrollment Protocol (SCEP) and enable GlobalProtect to use the SCEP configuration on Palo Alto Networks firewalls to validate that these client certificates (used to authenticate users) were positively issued to the authenticating device. When enabled, GlobalProtect blocks the session if the certificate does not match the device to which the certificate was issued. Both methods offer greater protection against unauthorized network access from known and unknown devices.
Certificate Selection by OID	You can now specify the certificate that GlobalProtect uses for authentication on Windows and Mac clients by entering the certificate object identifier (OID). By specifying the OID, GlobalProtect filters out all other certificates except for those with the matching OID.
Save Username Only Option	You can now enable GlobalProtect to save only a username when users log in to GlobalProtect. The new option provides an alternative to saving both the username and password. This option replaces the **Allow user to save password** option, which was available in PAN-OS 7.0. For upgrade information on this feature, see Upgrade/Downgrade Considerations.

New GlobalProtect Feature	Description
Use Address Objects in a GlobalProtect Gateway Client Configuration	You can now use an address object, which can include an IPv4 address or an FQDN, to define networking settings in a GlobalProtect gateway client configuration. IP address pools support address objects that define a single IP address, range of IP addresses, or IP netmask and access routes support address objects that define a single IP address or IP netmask. You can also define address objects in Panorama and deploy them with GlobalProtect settings to gateway devices.
Transparent Distribution of Trusted Root CAs for SSL Decryption	You can now easily and transparently install the trusted root certificate authority (CA) certificates required for SSL forward proxy decryption in a GlobalProtect portal configuration. For each CA certificate that you enable, the GlobalProtect portal automatically distributes the certificate to the GlobalProtect agent which installs it in the certificate store on GlobalProtect endpoints. The firewall uses these certificates to establish itself as a trusted third party to the session between the client and the server.
Maximum Internal Gateway Connection Retry Attempts	You can now configure the maximum number of retries when the GlobalProtect agent fails to connect to an internal gateway. By default, the agent does not retry the connection attempt when the internal gateway is temporarily down or unreachable. With this new feature, you can specify the number of retries by configuring the option in a GlobalProtect portal agent configuration.
GlobalProtect Notification Suppression	You can now suppress the bubble notification that GlobalProtect displays from the notification area (system tray). Each notification contains information about changes in the agent status. Suppressing the bubble notification allows the GlobalProtect agent to run more transparently and enables you to further customize the behavior of the GlobalProtect agent that runs on Windows clients.
Disable GlobalProtect Without Comment	For increased flexibility, you can now allow a user to disable the GlobalProtect app without providing a comment, passcode, or ticket number. In this release, you can configure the option as part of a GlobalProtect portal agent configuration. In earlier releases, this option was only available in the Windows registry or Mac global property list (plist). Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows registry or the Mac plist.

User-ID Features

New User-ID Feature	Description
User-ID Redistribution Enhancement	You can now relay user mapping information from one firewall to another in a sequence of up to ten hops instead of one. This increase in the relay sequence enables you to redistribute mapping information in a network that has hundreds of user identification sources or that has users who rely on local sources for authentication (for example, regional directory services) but who need access to remote resources (for example, global data center applications).
Ignore User List Configurable in Web Interface	For the PAN-OS integrated User-ID agent, you can now use the firewall web interface as an alternative to the CLI to configure the ignore user list, which specifies the user accounts that don't require IP address-to-username mapping (for example, kiosk accounts). Using the web interface is easier and reduces the chance of errors that might compromise the enforcement of user-based policies.

New User-ID Feature	Description
User Group Capacity Increase	On a PA-5060 or PA-7000 Series firewall with a single virtual system, you can now base policies on up to 3,200 distinct user groups instead of 640. This ensures continued security on networks that use a large number of groups to control access to resources.

Networking Features

New Networking Feature	Description
Failure Detection with BFD	Data centers and networks often require very fast detection of communication failures. The firewall now supports Bidirectional Forwarding Detection (BFD), a protocol that detects failures in the bidirectional path between an interface on the firewall and a configured BFD peer. The PAN-OS implementation of BFD allows you to configure BFD settings (such as transmit and receive intervals) per routing protocol or static route.
LACP and LLDP Pre-Negotiation for an HA Passive Firewall	An HA passive firewall can now negotiate LACP and LLDP before it becomes active. This pre-negotiation reduces failover times by eliminating the delays incurred by LACP or LLDP negotiations.
Binding a Floating IP Address to an HA Active-Primary Firewall	In an HA active/active configuration, you can now bind a floating IP address to the firewall in the active-primary state. Thus, on a failover, when the active-primary firewall (Peer A) goes down and the active-secondary firewall (Peer B) takes over as the active-primary peer, the floating IP address moves to Peer B. Traffic continues to go to Peer B, even when Peer A recovers and becomes the active-secondary device. This feature provides more control over how floating IP address ownership is determined as firewalls move between HA states. Prior to this feature, the floating IP address was bound to the firewall through its Device ID [0/1] and would follow the Device ID to which it was bound. Now, in mission-critical data centers, you can benefit from this feature in several ways: • You can have an active/active configuration so that you can do path monitoring out of both firewalls, yet the HA peers function like an active/passive configuration because traffic directed to the floating IP address always goes to the active-primary firewall. • The floating IP address does not move back and forth between HA devices if the active-secondary device flaps up and down. Therefore, traffic remains stable on the active-primary firewall. • You have control over which firewall owns the floating IP address, so you can keep new and existing sessions on the active-primary firewall. • You can verify a firewall is fully functional before you manually pass ownership of the floating IP address back to it.
Multicast Route Setup Buffering	You can now enable buffering of the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not yet exist for the corresponding multicast group. By default, the firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. You need to enable multicast route setup buffering only if your content servers are directly connected to the firewall and your custom application cannot withstand the first packet in the session being dropped.

New Networking Feature	Description
Per VLAN Spanning Tree (PVST+) BPDU Rewrite	When an interface on the firewall is configured for a Layer 2 deployment, the firewall now rewrites the inbound Port VLAN ID (PVID) number in a Cisco per-VLAN spanning tree (PVST+) bridge protocol data unit (BPDU) to the proper outbound VLAN ID number and forwards it out. This new default behavior in PAN-OS 7.1 allows the firewall to correctly tag Cisco proprietary Per VLAN Spanning Tree (PVST+) and Rapid PVST+ frames between Cisco switches in VLANs on either side of the firewall. Thus, spanning tree loop detection using Cisco PVST+ functions properly. There is no behavior change for other types of spanning tree.
Configurable MSS Adjustment Size	The Maximum Segment Size (MSS) adjustment size is now configurable so that you can adjust the number of bytes available for the IP and TCP headers in an Ethernet frame. You can expand the adjustment size beyond 40 bytes to accommodate longer IP and TCP headers. For example, if you are forwarding a packet through an MPLS network where multiple tags can be added to the packet, you may need to increase the number of bytes in the header.
DHCP Client Support on the Management Interface	The management interface on the firewall now supports DHCP client for IPv4, which allows the management interface to receive its IPv4 address from a DHCP server. The management interface also supports DHCP Option 12 and Option 61, which allow the firewall to send its hostname and client identifier, respectively, to a DHCP server.
Increase in Number of DHCP Servers per DHCP Relay Agent	In a DHCP relay agent configuration, each Layer 3 Ethernet or VLAN interface now supports up to eight IPv4 DHCP severs and eight IPv6 DHCP servers. This is an increase over the previous limit of four DHCP servers per interface per IP address family.
PA-3000 Series and PA-500 Firewall Capacity Increases	PA-3000 Series and PA-500 firewalls support more ARP entries, MAC addresses, and IPv6 neighbors than they supported in prior releases. Additionally, PA-3000 Series firewalls support more FIB addresses.
SSL/SSH Session End Reasons	The Session End Reason column in Traffic logs now indicates the reason for SSL/SSH session termination. For example, the column might indicate that a server certificate expired if you configured certificate expiration as a blocking condition for SSL Forward Proxy decryption. You can use SSL/SSH session end reasons to troubleshoot access issues for internal users requesting external services or for external users requesting internal services.
Fast Identification and Mitigation of Sessions that Overutilize the Packet Buffer	A new CLI command (`show running resource-monitor ingress-backlogs`) on any hardware-based firewall platform allows you to see the packet buffer percentage used, the top five sessions using more than two percent of the packet buffers, and the source IP addresses associated with those sessions. This information is very helpful when a firewall exhibits signs of resource depletion and starts buffering inbound packets because it is an indication that the firewall might be experiencing an attack. Another new CLI command (`request session-discard [timeout <x>] [reason <reason_string>] id <session_id>`) allows you to immediately discard a session without a commit.
FPP Optimization on PA-7080 Firewalls	In PAN-OS 7.1.4-h2 and later PAN-OS 7.1 releases, First Packet Processor (FPP) performance on the PA-7080 firewall is further optimized to enhance maximum session establishment rate

Decryption Features

New Decryption Features	Description
Transparent Certificate Distribution for SSL Forward Proxy	You can now use GlobalProtect to easily distribute the forward trust certificate required for SSL Forward Proxy decryption to client systems.
Perfect Forward Secrecy (PFS) Support with SSL Forward Proxy Decryption	Palo Alto Networks firewalls now support PFS when performing SSL Forward Proxy decryption. PFS ensures that data from the session undergoing SSL Forward Proxy decryption cannot later be retrieved in the event that server private keys are compromised. You can enforce Diffie-Hellman key exchange-based PFS (DHE) and/or elliptic curve Diffie-Hellman-based PFS (ECDHE) with SSL Forward Proxy.

VPN Features

New VPN Feature	Description
DES Support for Crypto Profiles	IKE gateways and IPSec tunnels now support Data Encryption Standard (DES) as an encryption algorithm in crypto profiles for a site-to-site VPN connection. DES support provides backward compatibility with legacy devices that do not use stronger encryption methods.

Panorama Features

New Panorama Feature	Description
Role Privileges for Commit Types	For custom Panorama administrator roles, you can now assign commit privileges by type (Panorama, device group, template, or Collector Group) instead of assigning one comprehensive commit privilege. This improves the security of Panorama, firewalls, and Log Collectors by providing more granular control over the types of configuration changes that each Panorama administrator can commit.
8TB Disk Support on the Panorama Virtual Appliance	You can now add a virtual disk of up to 8TB instead of 2TB on a Panorama virtual appliance that runs on a VMware ESXi server (version 5.5 or later) or on vCloud Air. This increased disk capacity enables Panorama to store more logs.

Hardware Features

New Hardware Feature	Description
PA-7000 Series Firewall Network Processing Cards with Double the Session Capacity	Two new Network Processing Cards (NPCs) are now available to double the session capacity of previously released NPCs. • **PA-7000-20GXM—**Doubles the memory of the PA-7000-20G NPC, enabling support for eight million sessions (up from four million). This NPC has twelve RJ-45 10/100/1000Mbps ports, eight SFP ports, and four SFP+ ports. • **PA-7000-20GQXM—**Doubles the memory of the PA-7000-20GQ NPC, enabling support for eight million sessions (up from four million). This NPC has twelve SFP+ ports and two QSFP ports. For example, installing ten PA-7000-20GXM NPCs in a PA-7080 firewall enables support for up to 80 million sessions. All PA-7000 Series NPCs are compatible with each other, so you can install any combination of them in a PA-7050 or PA-7080 firewall. You must upgrade the firewall to PAN-OS 7.1 before you install a PA-7000-20GXM or PA-7000-20GQXM NPC. For more information, refer to the PA-7000 Series Hardware Reference Guide.

Changes to Default Behavior

PAN-OS 7.1 has the following changes in default behavior.

You can also see CLI Changes in PAN-OS 7.1 and XML API Changes in PAN-OS 7.1.

- ▲ App-ID Changes
- ▲ Authentication Changes
- ▲ Decryption Changes
- ▲ GlobalProtect Changes
- ▲ Networking Changes
- ▲ URL Filtering Changes
- ▲ User-ID Changes
- ▲ Virtualization Changes
- ▲ WildFire Changes

App-ID Changes

PAN-OS 7.1 has the following changes in default behavior for App-ID features:

Feature	Change
Application defaults	When you configure a Security policy rule with the Application setting **Any** and the Service setting **application-default**, all applications are now permitted only on their standard ports as defined in Palo Alto Networks Applipedia. For example, if a Security policy rule allows any application traffic on the default application ports, the firewall will allow web-browsing traffic only on port 80 and SSH traffic only on port 22. In earlier PAN-OS release versions, the Service setting **application-default** was interpreted as **Any** when configured with the Application setting **Any**. You can replicate the behavior of earlier PAN-OS releases by changing rules with the Application setting **Any** and the Service setting **application-default** to include the Application setting **Any** and the Service setting **Any**. With all PAN-OS release versions, applications continue to be permitted only on their standard ports when the applications are explicitly defined in a rule (Application is not set to **Any**) and the Service setting is set to **application-default**.

Authentication Changes

PAN-OS 7.1 has the following changes in default behavior for authentication features:

Feature	Change
Hardware security modules	⚠ (PAN-OS 7.1.10 and later releases) To downgrade to a release earlier than PAN-OS 7.1.10, you must ensure that the master key is stored locally on Panorama or on the firewall, not on a hardware security module (HSM).

Decryption Changes

PAN-OS 7.1 has the following changes in default behavior for Decryption features:

Feature	Change
Decryption profiles	• (PAN-OS 7.1.10 and later releases) The firewall does not support SSL decryption of RSA keys that exceed 8Kb in size. You can either block connections to servers that use certificates with RSA keys exceeding 8Kb or skip SSL decryption for such connections. To block such connections, select **Objects > Decryption Profile**, edit the profile, select **SSL Decryption > SSL Forward Proxy**, and in the Unsupported Mode Checks section select **Block sessions with unsupported cipher suites**. To skip decryption for such connections, clear **Block sessions with unsupported cipher suites**. • (PAN-OS 7.1.6 and later releases) The maximum size of a server certificate chain for SSL traffic is now restricted to approximately 24KB. The Decryption profile does not exclude certificate chains larger than 24KB, and the firewall discards sessions using a certificate chain larger than 24KB. In releases earlier than PAN-OS 7.1.6, server certificate chains that exceed 16KB fail decryption and the Decryption profile excludes them as unsupported.

GlobalProtect Changes

PAN-OS 7.1 has the following changes in default behavior for GlobalProtect features:

Feature	Change
GlobalProtect portal agent	• The **Allow user to save password** option, which was available in PAN-OS 7.0 in a GlobalProtect portal agent configuration, is now deprecated and is superseded by the **Save User Credentials** setting in PAN-OS 7.1. After you upgrade the firewall or Panorama to PAN-OS 7.1, the setting is discarded. Because the default behavior—which allows GlobalProtect to save user credentials—is the same for both options, no additional configuration is required to retain this behavior. However, to enforce behavior other than the default—for example, to prevent GlobalProtect from saving credentials altogether or from saving the password only—you must manually configure the **Save User Credentials** option after upgrading to PAN-OS 7.1. • The **Authentication Modifier** option, which was available in PAN-OS 7.0 in a GlobalProtect portal agent configuration, is now deprecated by the **Authentication Override** options in PAN-OS 7.1. After you upgrade the firewall or Panorama to PAN-OS 7.1, any authentication modifier settings are discarded. Because the new **Authentication Override** options are disabled by default, to configure GlobalProtect portals and gateways to accept secure encrypted cookies, you must manually configure the new **Authentication Override** options in PAN-OS 7.1.

Networking Changes

PAN-OS 7.1 has the following changes in default behavior for networking features:

Feature	Change
VLAN tags	• In Layer 2 deployments, by default, the firewall rewrites the inbound VLAN tag in a Cisco per-VLAN spanning tree (PVST+) or Rapid PVST+ bridge protocol data unit (BPDU) to the correct outbound VLAN tag before forwarding the BPDU. In PAN-OS 7.0 and earlier releases, the firewall flooded the packets to the VLANs in the VLAN group without rewriting the tag, which disrupted Cisco PVST+. • The firewall has the following changes to how it handles the Priority Code Point (PCP) value in the VLAN tag field when forwarding the frame between different VLANs: • (PAN-OS 7.1.5 and later releases) A new CLI command (`set session pass-through-1q-pcp <yes|no>`) allows you to configure how the firewall handles the PCP value. By default, the firewall automatically unsets the PCP value when forwarding between VLANs, but you can use this new command if you need to preserve the PCP value in the VLAN tag field. • (PAN-OS 7.1.3 and 7.1.4 only) The firewall preserves the PCP value in the VLAN tag field by default when forwarding the frame.

Feature	Change
Floating IP addresses	(PAN-OS 7.1.4 and later releases) PA-5000 Series firewalls have an increased number of allowed virtual floating IP addresses in active/active configurations. With this change, the available floating IP addresses for each firewall model are as follows: • PA-5020 has 1024 floating IP addresses • PA-5050 has 2048 floating IP addresses • PA-5060 has 2048 floating IP addresses

URL Filtering Changes

PAN-OS 7.1 has the following changes in default behavior for URL Filtering features:

Feature	Change
External Dynamic Lists	In PAN-OS 7.0 and earlier versions, each firewall supported a maximum of 10 Dynamic Block Lists (of type IP address only) and each list could contain the maximum number of IP addresses supported by your firewall model minus 300; 300 IP addresses were reserved for internal use on the firewall and were deducted from the available limit. In PAN-OS 7.1, Dynamic Block Lists are called External Dynamic Lists. External Dynamic Lists can be of three types: IP address, Domain, or URL. On any firewall model, you can configure a maximum of 30 unique sources for external dynamic lists. While the firewall does not impose a limit on the number of lists of a specific type, the following limits are enforced: • IP address—The PA-5000 Series and the PA-7000 Series firewalls support a maximum of 150,000 total IP addresses; all other platforms support a maximum of 50,000 total IP addresses. No limits are enforced for the number of IP addresses per list. When the maximum supported IP address limit is reached on the firewall, the firewall generates a syslog message. • URL and domain—A maximum of 50,000 URLs and 50,000 domains are supported on each platform, with no limits enforced on the number of entries per list.
URL categories	In PAN-OS 7.1, the maximum number of custom categories supported per virtual system has increased from 50 to 500. The maximum number of shared custom categories on a firewall has increased from 50 to 100. All other limits are the same as in earlier PAN-OS versions. The maximum number of custom categories, across the shared location and all virtual systems enabled on the firewall, stays at 2,900.

User-ID Changes

PAN-OS 7.1 has the following changes in default behavior for User-ID features:

Feature	Change
Client probing	When performing client probing using Windows Management Instrumentation (WMI), the User-ID agent now excludes public IPv4 addresses by default (those public IP addresses outside the scope of RFC 1918 and RFC 3927). To enable WMI probing of public IPv4 addresses, you must add their subnetworks to the Include List of the User-ID agent.

Virtualization Changes

PAN-OS 7.1 has the following changes in default behavior for virtualization features:

Feature	Change
VM-Series license	(PAN-OS 7.1.7 and later releases) To deactivate a VM-Series license you must first install a license API key on your firewall or Panorama. For more information, see Virtualization Features.
AWS Marketplace	(PAN-OS 7.1.6 and later releases) All newly deployed instances of the BYOL and usage-based models of the VM-Series firewall (Bundle 1 and Bundle 2) available through the AWS Marketplace support the longer AWS instance ID format. These firewalls will have a longer serial number and a new CPU ID format.
VMware Service Manager	The VMware Service Manager configuration, which is required for deploying the VMware NSX edition firewall, changes in the following ways on upgrade: • The **VMware Service Manager** configuration on Panorama is separated from the Service Definition. • A new **VMware Service Definition** called Palo Alto Networks NGFW is created. This service definition includes a template, device group, link to the ova for the PAN-OS version, and auth codes that you had configured on the VMware service manager in the earlier version. Since a template was optional in the earlier versions, the template name you defined is used if you had created one, otherwise a default template called NSX_TPL is created for you. • A zone called Palo Alto Networks profile 1 is auto-generated within the template; the zone is enabled as **Service profile zone for NSX.** On a Template and Device Group Commit, the VM-Series firewalls will generate a pair of virtual wire subinterfaces (ethernet 1/1.2 and ethernet 1/2.2) and bind the pair to this zone.

WildFire Changes

PAN-OS 7.1 has the following changes in default behavior for WildFire features:

Feature	Change
Mac OS X file analysis	Palo Alto Networks firewalls running PAN-OS 7.1 and with the content release version 582 or later that are configured to forward Any file type for WildFire analysis, will automatically begin forwarding Mac OS X files. For details about Mac OS X file analysis and how to define the file types the firewall forwards for WildFire analysis, see Mac OS X File Analysis.

CLI Changes in PAN-OS 7.1

PAN-OS 7.1 has the following CLI changes, which also affect corresponding PAN-OS XML API requests. You can use the CLI in debug mode to view the corresponding XML API syntax for CLI commands. For changes that are specific to the XML API, see XML API Changes in PAN-OS 7.1.

- App-ID CLI Changes
- GlobalProtect CLI Changes
- Management CLI Changes
- Monitoring CLI Changes
- Networking CLI Changes
- Threat Prevention CLI Changes
- URL Filtering CLI Changes
- User-ID CLI Changes

App-ID CLI Changes

PAN-OS 7.1 has the following CLI changes for App-ID features:

Feature	Change

Application status	With the role-based access control enhancements, on firewalls enabled for multiple virtual systems, you must specify the target virtual system before you can view or set application status. The following commands have changed:
	• PAN-OS 7.0 and earlier releases:
	`request get-disabled-applications vsys <value>`
	`request get-application-status vsys <value> application <value>`
	`request set-application-status-recursive vsys <value> enable-dependent-apps <yes|no> application <value> status <enabled|disabled>`
	• PAN-OS 7.1 and later releases:
	First set the target vsys.
	`set system setting target-vsys <value>`
	Then enter the command to retrieve or set the application status.
	`request get-disabled-applications`
	`request get-application-status application <value>`
	`request set-application-status-recursive enable-dependent-apps <yes|no> application <value> status <enabled|disabled>`

GlobalProtect CLI Changes

PAN-OS 7.1 has the following CLI changes for GlobalProtect features:

Feature	Change

Two-factor authentication	With the introduction of two-factor authentication in GlobalProtect, a number of API requests have been changed. Use the CLI with the command `debug cli on` to see changes in the corresponding XML requests. Affected commands are within the following command hierarchy:
	`set global-protect global-protect-portal <name> satellite-config`
	`set global-protect global-protect-portal <name> client-config`
	`set global-protect global-protect-portal <name> portal-config`

Management CLI Changes

PAN-OS 7.1 has the following CLI changes for management features:

Feature	Change

API keys	(PAN-OS 7.1.7 and later releases) New commands enable you to manage API keys. These keys are required when performing secure credential operations, including VM-Series license deactivation. Refer to VM-Series License Deactivation API Key. Use the following commands to manage API keys:
	• To show the current API key:
	`request license api-key show`
	• To delete the current API key:
	`request license api-key delete`
	• To configure the API key:
	`request license api-key set key <key>`

Restarting processes	(PAN-OS 7.1.5 and later releases) New commands enable you to restart firewall processes (*bfd*, *cryptod*, *dhcpd*, *ikemgr*, *keymgr*, and *pppoed*) that previously required root access to restart:
	`debug software restart process bfd`
	`debug software restart process crypto`
	`debug software restart process dhcp`
	`debug software restart process ikemgr`
	`debug software restart process keymgr`
	`debug software restart process pppoe`

Content updates	(PAN-OS 7.1.3 and later releases) New commands enable you to check for application and threat content updates hourly and to verify the configuration:
	`debug management-server content hourly-check set enable`
	`debug management-server content hourly-check show`

Feature	Change
Operational modes	The maintenance mode menu for selecting the mode of operation changed: • **Firewall platforms**—The **Set CCEAL4 mode** menu is renamed to **Set FIPS-CC mode**. Additionally, the **Set FIPS mode** menu is removed • **Panorama virtual appliances, M-Series appliances, and WF-500 appliances**—The **Set CCEAL4 mode** menu is renamed to **Set FIPS-CC mode**. If your firewall is set to FIPS mode, you must change the mode of operation to CCEAL4 mode (using **Set CCEAL4 mode** menu option in maintenance mode) before you upgrade to a PAN-OS 7.0. or later release. See upgrade considerations for more details on upgrading a firewall that is set to FIPS mode. ⚠ When you change from FIPS mode to CCEAL4 mode, you lose all configuration settings so it is important to back up your configuration first and re-import it after you change modes (and before you upgrade). For information on changing to FIP-CC mode, refer to Certifications.

Decompression modes	Hardware-based and software-based decompression is supported on all Palo Alto Networks platforms (excluding VM-Series firewalls). Starting in PAN-OS 7.1, a hybrid mode (enabled by default) allows firewalls to dynamically switch from hardware-based decompression to software-based decompression when the hardware decompression engine is under a heavy load and then switch back when the load decreases. Prior to PAN-OS 7.1, you could manually switch between decompression modes but you could choose only one mode at a time: hardware (default) or software.
	You can modify this new setting (`zip mode auto`) so that the firewall performs only hardware-based decompression or software-based decompression as needed.
	• PAN-OS 7.0 and earlier releases:
	`set deviceconfig setting zip sw [yes|no]`
	• PAN-OS 7.1 and later releases:
	`set deviceconfig setting zip mode [sw | hw | auto]`
	New counters are also introduced to the `show system setting zip` command output to monitor the number of times that the firewall switches from hardware-based decompression to software-based decompression:
	• **Number of SW Forced Switchovers**—The number of times that the firewall forces a switchover to software-based decompression. A forced switchover can occur when the firewall is in hardware zip mode if the hardware decompression engine becomes unresponsive.
	• **Number of SW Automatic Switchovers**—The number of times the firewall has dynamically switched from hardware-based to software-based decompression when in automatic zip mode.

CPU monitoring	The following command now shows asterisks (*) instead of zeroes (0) when a corresponding CPU core load percentage is not currently being measured or cannot be measured: `show running resource-monitor` An asterisk may indicate potential issues such as a malfunction that causes packet processing to pause. When issues like this occur, the response repeatedly shows an asterisk instead of a number. It is normal for core 0 to always show an asterisk.

Monitoring CLI Changes

PAN-OS 7.1 has the following CLI changes for monitoring features:

Feature	Change

Log filtering	To view the results of a query, the request format has been updated to be uniform between firewalls and Panorama:
	• PAN-OS 7.0 and earlier releases:
	`show query id <1-4294967295>`
	• PAN-OS 7.1 and later releases:
	`show query result id <1-4294967295> skip <0-4294967295>`

Networking CLI Changes

PAN-OS 7.1 has the following CLI changes for networking features:

Feature	Change

VLANs	(PAN-OS 7.1.5 and later releases) A new command allows you to configure how the firewall handles the Priority Code Point (PCP) value in the VLAN tag field when forwarding the frame between different VLANs. By default, the firewall automatically unsets the PCP value when forwarding between VLANs for greater security. To address a requirement in a particular customer environment, you can configure the firewall to pass through the PCP value so that it is preserved on frame forwarding. Use the following command to configure this behavior, where the default value is no to disable PCP pass-through:
	`set session pass-through-1q-pcp <yes|no>`
	To view the PCP configuration, use the existing command to display VLANs:
	`show vlan all`
	The command output has the following updates associated with the PCP pass-through configuration:
	`pvst+ tag rewrite:                    enabled`
	`pvst+ native vlan id:                 1`
	`drop stp:                             disabled`
	`802.1Q PCP pass through:              disabled`

Feature	Change

Interfaces	- With the introduction of configurable maximum segment size (MSS) adjustment sizes, the request format to enable MSS adjustment has changed:
	- PAN-OS 7.0 and earlier releases:
	`set network interface ethernet <name> layer3 adjust-tcp-mss <yes|no>`
	`set network interface ethernet <name> layer3 units <name> adjust-tcp-mss <yes|no>`
	`set network interface vlan adjust-tcp-mss <yes|no>`
	`set network interface vlan units <name> adjust-tcp-mss <yes|no>`
	`set network interface loopback adjust-tcp-mss <yes|no>`
	`set network interface loopback units <name> adjust-tcp-mss <yes|no>`
	- PAN-OS 7.1 and later releases:
	`set network interface ethernet <name> layer3 adjust-tcp-mss enable <yes|no>`
	`set network interface ethernet <name> layer3 units <name> adjust-tcp-mss enable <yes|no>`
	`set network interface vlan adjust-tcp-mss enable <yes|no>`
	`set network interface vlan units <name> adjust-tcp-mss enable <yes|no>`
	`set network interface loopback adjust-tcp-mss enable <yes|no>`
	`set network interface loopback units <name> adjust-tcp-mss enable <yes|no>`
	- The `netstat` command has moved from the root level to within the `request` command hierarchy:
	- PAN-OS 7.0 and earlier releases:
	`netstat programs yes interface yes`
	- PAN-OS 7.1 and later releases:
	`request netstat programs yes interface yes`
	Additionally, use of the `request netstat programs` command option now requires superuser or superreader permissions.

Session settings	The CLI command to set the maximum number of multicast packets queued per session has changed. The new command updates the configuration instead of running an operational command. This change, which persists even if the firewall is reset, now requires you to commit your configuration changes:
	- PAN-OS 7.0 and earlier releases:
	`set session max-pending-mcast-pkts-per-session <0-2000>`
	- PAN-OS 7.1 and later releases:
	`set deviceconfig setting session max-pending-mcast-pkts-per-session <1-2000>`

Threat Prevention CLI Changes

PAN-OS 7.1 has the following CLI changes for threat prevention features:

Feature	Change

Anti-Spyware profiles	With the new ability to specify intelligence sources through a list on an external domain, you must now specify the list. Example changes in the CLI follow:
	• PAN-OS 7.0 and earlier releases:
	`show profiles spyware <name> botnet-domains action`
	`show profiles spyware <name> botnet-domains action alert`
	`show profiles spyware <name> botnet-domains action allow`
	`show profiles spyware <name> botnet-domains action block`
	`show profiles spyware <name> botnet-domains action sinkhole`
	• PAN-OS 7.1 and later releases:
	`show profiles spyware <name> botnet-domains lists <name> action`
	`show profiles spyware <name> botnet-domains lists <name> action alert`
	`show profiles spyware <name> botnet-domains lists <name> action allow`
	`show profiles spyware <name> botnet-domains lists <name> action block`
	`show profiles spyware <name> botnet-domains lists <name> action sinkhole`

URL Filtering CLI Changes

PAN-OS 7.1 has the following CLI changes for URL Filtering features:

Feature	Change

External Dynamic Lists	When indicating an hourly polling time for external block lists (now called *external dynamic lists*), you can no longer indicate a specific minute within the hour. The change in the CLI is as follows:
	• **PAN-OS 7.0 and earlier releases:**
	`set external-list <name> recurring hourly at <value>`
	• **PAN-OS 7.1 and later releases:**
	`set external-list <name> recurring hourly`

User-ID CLI Changes

PAN-OS 7.1 has the following CLI changes for User-ID features:

<table>
<tr><th>Feature</th><th>Change</th></tr>
<tr><td>Username-to-group mapping</td><td>The following User-ID configuration commands, used to retrieve the list of groups and the corresponding list of members from an LDAP server, now require you to specify the virtual system to which the LDAP server profile belongs:
• PAN-OS 7.0 and earlier releases:
`show user group-mapping naming-context server <ip/netmask>|<value> server-port <1-65535> use-ssl <yes|no> is-active-directory <yes|no> proxy-agent <ip/netmask>|<value> proxy-agent-port <1-65535>`
`show user group-selection use-ssl <yes|no> base <value> bind-dn <value> bind-password <value> name-attribute <value> group-object <value> container-object <value> filter <value> search-scope <one|subtree> proxy-agent <ip/netmask>|<value> proxy-agent-port <1-65535> force <yes|no> server [<server1> <server2>...]`<br>`show user group-selection use-ssl <yes|no> base <value> bind-dn <value> bind-password <value> name-attribute <value> group-object <value> container-object <value> filter <value> search-scope <one|subtree> proxy-agent <ip/netmask>|<value> proxy-agent-port <1-65535> force <yes|no> server-port [<server-port1> <server-port2>...]`<br>• PAN-OS 7.1 and later releases:<br>`show user group-mapping naming-context server <ip/netmask>|<value> sp_vsys_id <value> server-port <1-65535> use-ssl <yes|no> is-active-directory <yes|no> proxy-agent <ip/netmask>|<value> proxy-agent-port <1-65535>`<br>`show user group-selection sp_vsys_id <value> use-ssl <yes|no> base <value> bind-dn <value> bind-password <value> name-attribute <value> group-object <value> container-object <value> filter <value> search-scope <one|subtree> proxy-agent <ip/netmask>|<value> proxy-agent-port <1-65535> force <yes|no> server [<server1> <server2>...]`<br>`show user group-selection sp_vsys_id <value> use-ssl <yes|no> base <value> bind-dn <value> bind-password <value> name-attribute <value> group-object <value> container-object <value> filter <value> search-scope <one|subtree> proxy-agent <ip/netmask>|<value> proxy-agent-port <1-65535> force <yes|no> server-port [<server-port1> <server-port2>...]`</td></tr>
</table>

XML API Changes in PAN-OS 7.1

The PAN-OS 7.1 XML API has the following changes:

Feature	Change

User-ID	(PAN-OS 7.1.5 and later releases) The firewall has the following changes in how it times out IP address and user mapping information registered using the XML API. Unless you explicitly specify a timeout value in the API request, the firewall inherits the User-ID timeout value configured on the firewall (the **Enable User ID Timeout** value in **Device > User Identification > User Mapping > Cache**).
	In releases earlier than PAN-OS 7.1.5, when you did not specify a timeout value, the firewall treated the value as 0, which meant that the IP address and user mapping never expired. If you want to preserve the same behavior and ensure that the mapping never expires, you must explicitly set the timeout value to 0 as shown in the following API request:
	`<uid-message><version>1.0</version><type>update</type><payload><login>`
	`<entry name="domain\name2" ip="1.1.1.2" timeout="0"/>`
	`</login></payload></uid-message>`

Error codes	Certain PAN-OS XML API configuration requests now return a different API error code to accurately indicate that the object specified by the XPath does not exist. Affected requests include `type=config` with `action=delete` and `type=config` with `action=get`.
	• **PAN-OS 7.1 and later releases:**
	`<response code="7" status="success"><msg>Object doesn't exist</msg></response>`
	• **PAN-OS 7.0 and earlier releases (action=delete):**
	`<response code="20" status="success"><msg>Object doesn't exist</msg></response>`
	• **PAN-OS 7.0 and earlier releases (action=get):**
	`<response code="19" status="success"><msg>Object doesn't exist</msg></response>`

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.

Associated Software Versions

The following minimum software versions are supported with PAN-OS 7.1. To see a list of the next-gen firewall models that support PAN-OS 7.1, see the Palo Alto Networks® Compatibility Matrix.

Palo Alto Networks Software	Minimum Supported Version with PAN-OS 7.1
Panorama	7.1
User-ID Agent	7.0
Terminal Server Agent	7.0
GlobalProtect Agent	2.3
Content Release Version	564

Limitations

The following table includes limitations associated with the PAN-OS 7.1 release.

Issue ID	Description
PAN-76757	If the firewall collects IP address-to-username mappings by monitoring numerous servers at short intervals (**Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Server Monitor > Server Log Monitor Frequency**) in networks with high user log-in rates, the best practice is to deploy Windows-based User-ID agents instead of the PAN-OS integrated User-ID agent. Using Windows-based User-ID agents avoids the risk of the firewall running out of memory while querying the servers.

Known Issues

The following list describes WildFire Known Issues, GlobalProtect Known Issues, and Firewall and Panorama Known Issues in the PAN-OS 7.1 release:

> 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.
>
> Starting with PAN-OS 7.1.5, these release notes identify all unresolved known issues using new issue ID numbers that include a product-specific prefix. Known issues for earlier releases use both their new issue IDs and their original issue IDs (in parentheses).

Issue ID	Description
WildFire Known Issues	
WF500-4229	The WF-500 appliance is not supported with PAN-OS 7.1.1. However, a WF-500 appliance that is running PAN-OS 7.1.0 (or 7.1.2 and later releases) is compatible with firewalls running any PAN-OS 7.1 release version (including PAN-OS 7.1.1).
WF500-3062 (95815) This issue is now resolved.	When PAN-OS 7.1 was first released, firewalls could not forward files to the WildFire Japan cloud for analysis. This issue is resolved for all PAN-OS 7.1 releases due to an update to the WildFire Japan cloud in August 2016.
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 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 **log details**, and then clicking the **WildFire Analysis Report** tab.
GlobalProtect Known Issues	
GPC-2742 (88933)	If you configure GlobalProtect portals and gateways to use client certificates and LDAP as two factors of authentication, Chromebook users that are running Chrome OS 47 or later versions can encounter excessive prompts to select a client certificate. **Workaround**: To prevent excessive prompts, configure a policy in the Google Admin console to specify the client certificate and deploy that policy to your managed Chromebooks: 1. Log in to the Google Admin console (https://admin.google.com) and select **Device management > Chrome management > User settings**. 2. In the Client Certificates section, enter the following URL pattern to **Automatically Select Client Certificate for These Sites**: `{"pattern": "https://[*.]", "filter":{}}` 3. Click **Save**. The Google Admin console deploys the policy to all devices within a few minutes.

Issue ID	Description
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** > *<gateway-config>* > **Agent** > **Client Settings** > *<client-settings-config>* > **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.
GPC-1517 (56434)	For the GlobalProtect app to access an MDM server through a Squid proxy, you must add the MDM server SSL access ports to the proxy server allow list. For example, if the SSL access port is 8443, add `acl SSL_ports port 8443` to the allow list.
Firewall and Panorama Known Issues	
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 7.1 release. **Workaround**: On PA-7000 Series firewalls running a PAN-OS 7.1 release, run the `debug skip-condor-reports no` command and then the `debug software restart process reportd` command to allow Panorama 8.0 to successfully query these firewalls. ⚠ Do not use this workaround if you use Panorama 8.0 to manage a PA-7000 Series firewall that is running a PAN-OS 7.0 release (known issue 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-75044	As of PAN-OS 7.1.9, the PA-200 firewalls no longer store the previous WildFire content package after a WildFire content update. As a result, the option to revert to the previous WildFire package is no longer available on the web interface. However, the CLI command for this task (`request wildfire downgrade install previous`) was not removed and now results in an error message (`downgrade job failed`).
PAN-75005 This issue is now resolved. See PAN-OS 7.1.9 Addressed Issues.	Loading a configuration other than running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release removes authentication profiles from GlobalProtect portals and gateways, which causes an auto-commit failure. **Workaround:** Select running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release.
PAN-71765	In PAN-OS 7.1.7, deactivating a VM-Series firewall from Panorama completes successfully, but the web interface does not update to show that deactivation is complete. **Workaround:** View deactivation status from Managed Devices (**Panorama > Managed Devices**).
PAN-71217	The Panorama log collector does not support the server-verification CLI configuration, thereby preventing you from using the CLI to install content and software updates in a secure manner. **Workaround:** Use the log collector CLI command **request license api-key delete** and then install content and software updates from Panorama.

Issue ID	Description
PAN-71215 This issue is now resolved. See PAN-OS 7.1.8 Addressed Issues.	In PAN-OS 7.1.7, when deactivating a VM-Series firewall from Panorama, if Panorama has the **Verify Update Server Identity** setting enabled (**Panorama > Setup > Services > Verify Update Server Identity**), but the firewall has the setting disabled (**Device > Setup > Services**), deactivation on the firewall does not complete successfully and the firewall becomes unreachable. **Workaround:** Ensure Panorama and the VM-Series firewall both have the **Verify Update Server Identity** setting enabled before deactivating the firewall.
PAN-70323 This issue is now resolved. See PAN-OS 7.1.9 Addressed Issues.	Firewalls running in FIPS-CC mode do not allow import of SHA-1 CA certificates even when the private key is not included; instead, firewalls display the following error: `Import of <cert name> failed. Unsupported digest or keys used in FIPS-CC mode.`
PAN-69874	(PAN-OS 7.1.5 and later releases only) When the PAN-OS XML API sends user mappings with no timeout value to a firewall that has the **Enable User Identification Timeout** option disabled, the firewall assigns the mappings a timeout of 60 minutes instead of never.
PAN-69340 This issue is now resolved. See PAN-OS 7.1.8 Addressed Issues.	When you use a license authorization code (capacity license or a bundle) to bootstrap a VM-Series firewall, the capacity license is not applied. This issue occurs because the firewall does not reboot after the license is applied. **Workaround:** Use the `request restart software` CLI command or reboot the firewall manually to activate the session capacity for the VM-Series model.
PAN-69141	On PA-7000 Series firewalls and Panorama Log Collectors, log collection processes consume excess memory and do not process logs as expected. This issue occurs when DNS response times are slow and scheduled reports contain fields that require DNS lookups. **Workaround:** Use the `debug management-server report-namelookup disable` CLI command to disable DNS lookups for reporting purposes.
PAN-67987	The GlobalProtect agent fails to connect using a client certificate if the intermediate CA is signed using the ECDSA hash algorithm.
PAN-67079 This issue is now resolved. See PAN-OS 7.1.7 Addressed Issues.	In PAN-OS 7.1.6, SSL sessions are discarded if the server certificate chain size exceeds 23KB. See Changes to Default Behavior for more information about this issue. **Workaround:** Exclude the affected site from decryption. Refer to live.paloaltonetworks.com/t5/Learning-Articles/How-to-Exclude-a-Site-from-SSL-Decryption/ta-p/56738.
PAN-63908	SSH sessions are incorrectly subjected to a URL category lookup even when SSH decryption is not enabled. As a result, SSH traffic is blocked when you enable forward proxy and configure a deny rule to match all traffic whose URL category is `Unknown`.
PAN-62453	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.

Issue ID	Description
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-59614 (98576)	In PAN-OS 7.1 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.
PAN-59298 (98164) This issue is now resolved. See PAN-OS 7.1.4 Addressed Issues.	If you delete the proxy server configuration on the firewall for the AutoFocus service, the configuration remains. **Workaround:** Use the `request restart software` CLI command or reboot the firewall to clean up the proxy server configuration.
PAN-59258 (98112) This issue is partially resolved in PAN-OS 7.1.4. See PAN-OS 7.1.4 Addressed Issues. This issue is fully resolved in PAN-OS 7.1.5. See PAN-OS 7.1.5 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-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-57629 (95846) This issue is now resolved. See PAN-OS 7.1.4 Addressed Issues.	Deleting the default administrator account on a VM-Series firewall in AWS causes the firewall to go into maintenance mode. This occurs because, to reboot successfully, the firewall requires the SSH key associated with the administrator account (the private key—`ssh-key`—used to provision the firewall in AWS).
PAN-57546 (95723) This issue is now resolved. See PAN-OS 7.1.4 Addressed Issues.	If you configure the GlobalProtect portal or gateway to authenticate using an authentication sequence and then specify a domain\user in the User/User Group settings of an agent configuration, authentication using secure encrypted cookies will fail.
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.

Issue ID	Description
PAN-56820 (94695) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	By default, the **AutoFocus URL** in the AutoFocus settings (**Device** > **Setup** > **Management**) is pre-configured with the correct URL for connecting to AutoFocus but the firewall will fail to connect to AutoFocus if you don't manually re-enter the URL. This issue occurs only when you initially configure AutoFocus settings (for example, after performing a factory reset of the firewall or after upgrading to PAN-OS 7.1). **Workaround**: When initially enabling AutoFocus threat intelligence on the firewall, you must delete the default **AutoFocus URL** and manually re-enter the address (`https://autofocus.paloaltonetworks.com:10443`).
PAN-56303 (93882) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	The VM-Series for Azure is supported in the Azure Resource Manager (ARM) environment only. You cannot export the VM-Series firewall or its VHD disk image from Azure and deploy it in a local or private data center. Also, you cannot re-import a VM-Series firewall or its VHD disk image into the ARM environment.
PAN-56217 (93752)	You cannot configure multiple DNS proxy objects that specify for the firewall to listen for DNS requests on the same interface (**Network** > **DNS Proxy** > **Interfaces**). If multiple DNS proxy objects are configured with the same interface, only the first DNS proxy object settings are applied. **Workaround**: If there are DNS proxy objects configured with the same interface, you must modify the DNS proxy objects so that each object specifies unique interfaces: • To modify a DNS proxy object that specifies only one interface, delete the DNS proxy object and reconfigure the object with an interface that is not shared among any other objects. • To modify a DNS proxy object configured with multiple interfaces, delete the interface that is shared with other DNS proxy objects. Click **OK** to save the modified object and **Commit**.
PAN-55825 (93097)	Performing an AutoFocus remote search that is targeted to a PAN-OS firewall or Panorama does not work correctly when the search condition contains a single or double quotation mark.
PAN-55754 (92979) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	The **Administrator Use Only** option (**Template** > **Device** > **Radius Profile**) is not available in PAN-OS 7.1.0 or PAN-OS 7.1.1.
PAN-55472 (92472) This issue is now resolved. See PAN-OS 7.1.4 Addressed Issues.	During the connection of a satellite to the GlobalProtect gateway, the Online Certificate Status Protocol (OCSP) verification for the GlobalProtect certificate fails because the OCSP response does not contain the signature certificate.
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-55253 (92094)	The firewall does not display the SaaS Application Usage report (**Monitor** > **PDF Reports** > **SaaS Application Usage**) if you **Close** the job execution status dialog (appears when you click **Run Now** to generate a SaaS report) and move to another tab and continue to **Commit** changes before the SaaS report finishes generating.

Issue ID	Description
PAN-55203 (92015)	When you change the reporting period for a scheduled report, such as the SaaS Application Usage PDF report, the report can have incomplete or no data for the reporting period. **Workaround**: If you need to change the reporting period for any scheduled report, create a new report for the desired time period instead of modifying the time period on an existing report.
PAN-55121 (91885) This issue is now resolved. See PAN-OS 7.1.4 Addressed Issues.	If you create a log filter by clicking a value in the Destination Country or Source Country column of a log page (such as the **Monitor** > **Logs** > **Traffic** page), the filter does not work because the filter string uses the country name instead of the country code. This issue occurs only when the value is a country; the filter works for other types of regions (such as city names). **Workaround**: Manually change the country name to the country code in the filter string (for example, change `United States to US`).
PAN-55019 (91726) This issue is now resolved. See PAN-OS 7.1.3 Addressed Issues.	If a call manager or SIP proxy is in a different zone than either the called or the calling party, using the hold and resume feature can result in one-way audio. **Workaround**: If using NAT, configure the call manager and local phone in the same zone.
PAN-54806 (91395) This issue is now resolved with a workaround. See PAN-OS 7.1.2 Addressed Issues.	Simultaneous transfer of large files from two different SMB servers over a GlobalProtect connection from a Windows 8 client causes the connection to fail. **Workaround**: In PAN-OS 7.1.2 and later releases, enable Heuristics on Windows 8 clients or set the tunnel interface MTU size to 1,300 to avoid this issue.
PAN-54660 (91171) This issue is now resolved. See PAN-OS 7.1.3 Addressed Issues.	When the firewall is processing a high volume of BFD sessions for routing peers that use BGP, OSPF or RIP, and the firewall is also processing a high volume of packets that belong to existing sessions and are not offloaded, the BFD sessions to those peers will flap when the firewall receives a content update.
PAN-54611 (91086) This issue is now resolved. See PAN-OS 7.1.3 Addressed Issues.	There is an issue where PA-7000 Series firewalls experience BGP disconnections because the firewall fails to send keepalive messages to neighbors within specified timers.
PAN-54606 (91079) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	An ungraceful reboot on a VM-Series firewall causes Dynamic IP address information to get out of sync.
PAN-54319 (90596) This issue is now resolved. See PAN-OS 7.1.3 Addressed Issues.	The FPGA intermittently fails to initialize on PA-5000 Series firewalls.
PAN-54254 (90496)	In Traffic logs, the following session end reasons for Captive Portal or a GlobalProtect SSL VPN tunnel indicate the incorrect reason for session termination: decrypt-cert-validation, decrypt-unsupport-param, or decrypt-error.
PAN-54153 (90326) This issue is now resolved. See PAN-OS 7.1.3 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 7.1.3 Addressed Issues.	Decrypted SSH sessions are not mirrored to the decrypt mirror interface as expected.
PAN-53897 (89925) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	Tarball images for bootstrapping firewalls that are created using a Mac OS (BSD-based tar format) are incompatible with the Debian-based tar format used by PAN-OS firewalls. **Workaround**: Use a Windows system to create a tarball image that is compatible with the firewalls.
PAN-53825 (89818)	For the VM-Series NSX edition firewall, when you add or modify an NSX service profile zone on Panorama, you must perform a Panorama commit and then perform a device group commit with the **Include Device and Network Templates** option selected. To successfully redirect traffic to the VM-Series NSX edition firewall, you must perform both a **Template** and a **Device Group** commit when you modify the zone configuration to ensure that the zones are available on the firewall.
PAN-53663 (89552)	When you open the SaaS Application Usage Report (**Monitor** > **PDF Reports** > **SaaS Application Usage**) on multiple tabs in a browser, each for a different virtual system (vsys), and you attempt to export PDFs from each tab, only the first request is accurate; all successive attempts will result in PDFs that are duplicates of the first report. **Workaround**: Export only one PDF at a time and wait for that export process to finish before you trigger the next export request.
PAN-53601 (89460)	Panorama running on an M-500 appliance cannot connect to a SafeNet Network or Thales Nshield Connect hardware security module (HSM).
PAN-51969 (86666)	On the NSX Manager, when you unbind an NSX Security Group from an NSX Security Policy rule, the dynamic tag and registered IP address are updated on Panorama but are not updated on the VM-Series firewalls. **Workaround**: To push the Dynamic Address Group updates to the VM-Series firewalls, you need to manually synchronize the configuration with the NSX Manager. (**Panorama** > **VMware Service Manager**, and select **NSX Config-Sync**).
PAN-51952 (86640)	If a security group overlap occurs in an NSX Security policy where the same security group is weighted with a higher and a lower priority value, the traffic may be redirected to the wrong service profile (VM-Series firewall instance). This issue occurs because an NSX Security policy with a higher weight does not always take precedence over a policy with a lower weight. **Workaround**: Make sure that members that are assigned to a security group are not overlapping with another security group and that each security group is assigned to a unique NSX Security policy rule. This allows you to ensure that NSX Security policy does not redirect traffic to the wrong service profile (VM-Series firewall).
PAN-51870 (86501)	When using the CLI to configure the management interface as a DHCP client, the commit fails if you do not provide all four DHCP parameters in the command. For a successful commit when using the `set deviceconfig system type dhcp-client` command, you must include each of the following parameters: `accept-dhcp-domain`, `accept-dhcp-hostname`, `send-client-id`, and `send-hostname`.
PAN-51869 (86500)	Canceling pending commits does not immediately remove them from the commit queue. The commits remain in the queue until PAN-OS dequeues them.

Issue ID	Description
PAN-51673 (86159)	BFD sessions are not established between two RIP peers when there are no RIP advertisements. **Workaround**: Enable RIP on another interface to provide RIP advertisements from a remote peer.
PAN-51216 (85458)	The NSX Manager fails to redirect traffic to the VM-Series firewall when you define new Service Profile zones for NSX on Panorama. This issue occurs intermittently on the NSX Manager when you define security rules to redirect traffic to the new service profiles that are available for traffic introspection and results in the following error: `Firewall configuration is not in sync with NSX Manager. Conflict with Service Profile Oddhost on service (Palo Alto Networks NGFW) when binding to host<name>.`
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 PAN-OS 7.0 or later releases. **Workaround**: Enable FIPS and Common Criteria support on all Palo Alto Networks firewalls and appliances before you upgrade to a PAN-OS 7.0 or later release.
PAN-51122 (85315)	For the VM-Series firewall, if you manually reset a heartbeat failure alarm on the vCenter server to indicate that the VM-Series firewall is healthy (change color to green), the vCenter server does not trigger a heartbeat failure alarm again.
PAN-50973 (85086)	FIPS-CC mode is not supported on the VM-Series firewall on Microsoft Hyper-V. Although the option for FIPS-CC mode is displayed in the maintenance mode menu, you cannot enable this option.
PAN-50677 (84641) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	The firewall does not update some processes as expected (such as *mgmtsrvr*, *reportd*, *logd*, and *pan_log_receiver*) when you specify a new DNS server (**Device** > **Setup** > **Services** [> **Global**]), which causes the firewall to continue forwarding some DNS requests to the previously configured DNS server instead of the current one.
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`.
PAN-50641 (84569)	Enabling or disabling BFD for BGP or changing a BFD profile that a BGP peer uses causes BGP to flap.
PAN-50197 (83722) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	Destination-based service routes do not work for RADIUS authentication servers. **Workaround**: Use service-specific service routes instead of destination-based service routes for RADIUS authentication servers.

Issue ID	Description
PAN-50186 (83702)	WildFire Analysis reports do not display as expected in the **WildFire Analysis Report** tab (**Monitor** > **Logs** > **WildFire Submissions** > **Detailed Log View**) on PA-7000 Series firewalls running PAN-OS 7.0.2 and later releases. **Workaround**: Use the WildFire portal (https://wildfire.paloaltonetworks.com) or the WildFire API to retrieve WildFire Analysis reports.
PAN-50038 (83446)	From the CLI, when you enable jumbo frames on a VM-Series firewall in AWS, the maximum transmission unit (MTU) size on the interfaces does not increase. The MTU on each interface remains at a maximum value of 1500 bytes.
PAN-48565 (80589)	The VM-Series firewall on Citrix SDX does not support jumbo frames.
PAN-48456 (80387)	IPv6-to-IPv6 Network Prefix Translation (NPTv6) is not supported when configured on a shared gateway.
PAN-48346 (80177) This issue is now resolved. See PAN-OS 7.1.2 Addressed Issues.	The URL block page does not display as expected when proxied requests from client use CONNECT method.
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-47073 (77850)	Web pages using the HTTP Strict Transport Security (HSTS) protocol sometimes do not display properly for end users. **Workaround**: End users must import an appropriate forward-proxy-certificate for their browsers.
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)	On a firewall with multiple virtual systems, if you add an authentication profile to a virtual system and give the profile the same name as an authentication sequence in Shared, reference errors occur. The same errors occur if the profile is in Shared and the sequence with the same name is in a virtual system. **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.
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 a high availability (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 PAN-OS 7.0 or later releases.

Issue ID	Description
PAN-43000 (71624)	Vulnerability detection of SSLv3 fails when SSL decryption is enabled. This occurs when you attach a Vulnerability Protection profile (that detects SSLv3—CVE-2014-3566) to a Security policy rule and that Security policy rule and an SSL Decryption policy rule are configured on the same virtual system in the same zone. After performing SSL decryption, the firewall sees decrypted data and no longer sees the SSL version number. In this case, the SSLv3 vulnerability is not identified. **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-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.
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-40130 (66976)	In the WildFire Submissions logs, the email recipient address is not correctly mapped to a username when configuring LDAP group mappings that are pushed in a Panorama template.
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.

Issue ID	Description
PAN-39501 (65824)	Unused NAT IP address pools are not cleared after a single commit, so a commit fails if the combined cache of unused pools, existing used pools, and new pools exceeds the memory limit. **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 PAN-OS 6.0 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 running PAN-OS 6.0.3 or an earlier PAN-OS 6.0 release to a PAN-OS 6.0.4 or later release before pushing a configuration to the devices.
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.
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-37127 (59749)	On the Panorama web interface, the **Policies** > **Security** > **Post Rules** > **Combined Rules Preview** window does not display post rules and local rules for managed devices.
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 configuration, 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-36728 (58833)	In some scenarios, traffic from newly added guests or virtual machines is not steered to the VM-Series NSX edition firewall even when the guests belong to a Security Group and are attached to a Security Policy that redirects traffic to that VM-Series firewall. **Workaround**: Reapply the Security Policy on the NSX Manager.

Issue ID	Description
PAN-36727 (58832)	A VM-Series firewall on an ESXi host fails to deploy with an error message: `Invalid OVF Format in Agent Configuration.` **Workaround**: Use the following command to restart the ESX Agent Manager process on the vCenter Server: `/etc/init.d/vmware-vpxd tomcat-restart`.
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-36394 (58170)	When the datastore is migrated for a guest, all current sessions are no longer steered to the VM-Series firewall. However, all new sessions are secured properly.
PAN-36393 (58168)	When deploying the VM-Series firewall, the Task Console displays `Error while enabling agent. Cannot complete the operation. See the event log for details.` This error displays even for a successful deployment. You can ignore the message if the VM-Series firewall is successfully deployed.
PAN-36333 (58049)	The Service dialog for adding or editing a service object in the web interface displays the incorrect port range for both source and destination ports: `1-65535`. The correct port range is `0-65535` and specifying port number `0` for either a source or destination port is successful.
PAN-36289 (57954)	If you deploy the VM-Series firewall and then assign the firewall to a template, the change is not recorded in the bootstrap file. **Workaround**: Delete the Palo Alto Networks NGFW Service on the NSX Manager, and verify that the template is specified on **Panorama** > **VMware Service Manager**, register the service, and re-deploy the VM-Series firewall.
PAN-36088 (57614)	When an ESXi host is rebooted or shut down, the functional status of the guests is not updated. Because the IP address is not updated, the dynamic tags do not accurately reflect the functional state of the guests that are unavailable.
PAN-36049 (57533)	The vCenter Server/vmtools displayed the IP Address for a guest incorrectly after vlan tags were added to an Ethernet port. The display did not accurately show the IP addresses associated with the tagged Ethernet port and the untagged Ethernet port. This issue was seen on some Linux OS versions such as Ubuntu.
PAN-35903 (57265)	When you edit a traffic introspection rule (to steer traffic to the VM-Series firewall) on the NSX Manager, an `invalid (tcp) port number` error—or `invalid (udp) port number` error—displays when you remove the destination (TCP or UDP) port. **Workaround**: Delete the rule and add a new one.

Issue ID	Description
PAN-35875 (57205)	When defining traffic introspection rules (to steer traffic to the VM-Series firewall) on the NSX Manager, either the source or the destination for the rule must reference the name of a Security Group; you cannot create a rule from any to any Security Group. **Workaround**: To redirect all traffic to the VM-Series firewall, you must create a Security Group that includes all the guests in the cluster. Then you can define a security policy that redirects traffic from and to the cluster so that the firewall can inspect and enforce policy on the east-west traffic.
PAN-35874 (57203)	Duplicate packets are being steered to the VM-Series firewall. This issue occurs if you enable distributed vSwitch for steering in promiscuous mode. **Workaround**: Disable promiscuous mode.
PAN-34966 (55586)	On a VM-Series NSX edition firewall, when adding or removing a Security Group (Container) that is bound to a Security Policy, Panorama does not get a dynamic update of the added or removed Security Group. **Workaround**: On **Panorama** > **VMware Service Manager**, click **Synchronize Dynamic Objects** to initiate a manual synchronization to get the latest update.
PAN-34855 (55393)	On a VM-Series NSX edition firewall, Dynamic Tags (update) do not reflect the actual IP address set on the guest. This issue occurs because the vCenter Server cannot accurately view the IP address of the guest.
PAN-33316 (52361)	Adding or removing ports on the Citrix SDX server after deploying the VM-Series firewall can cause a configuration mismatch on the firewall. To avoid the need to reconfigure the interfaces, consider the total number of data ports that you require on the firewall and assign the relevant number of ports on the SDX server when deploying the VM-Series firewall. For example, if you assign ports 1/3 and 1/4 on the SDX server as data interfaces on the VM-Series firewall, the ports are mapped to eth1 and eth2. If you then add port 1/1 or 1/2 on the SDX server, eth1 will be mapped to 1/1 or 1/2, eth2 will be mapped to 1/3 and eth3 to1/4. If ports 1/3 and 1/4 were set up as a virtual wire, this remapping will require you to reconfigure the network interfaces on the firewall.
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.
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-29411 (45424)	In some configurations, when you switch context from Panorama and access the web interface of a managed device, you are unable to upgrade the PAN-OS software image. **Workaround**: Use the **Panorama** > **Device Deployment** > **Software** tab to deploy and install the software image on the managed device.

Issue ID	Description
PAN-29385 (45391)	You cannot configure the management IP address on an M-100 appliance while it is operating as the secondary passive peer in an HA pair. **Workaround**: To set the IP address for the management interface, you must suspend the active Panorama peer, promote the passive peer to active state, change the configuration, and then reset the active peer to active state.
PAN-29053 (44937)	By default, the hostname is not included in the IP header of syslog messages sent from the firewall. However, some syslog implementations require this field to be present. **Workaround**: Enable the firewall to include the IP address of the firewall as the hostname in the syslog header by selecting **Send Hostname in Syslog** (**Device** > **Setup**).
PAN-28794 (44571)	If a Panorama Log Collector MGT port is configured with an IPv4 address and you want to have only an IPv6 address configured, you can use the Panorama web interface to configure the new IPv6 address but you cannot use Panorama to remove the IPv4 address. **Workaround**: Configure the MGT port with the new IPv6 address and then apply the configuration to the Log Collector and test connectivity using the IPv6 address to ensure that you do not lose access when you remove the IPv4 address. After you confirm the Log Collector is accessible using the IPv6 address, go to the CLI on the Log Collector and remove the IPv4 address (using the `delete deviceconfig system ip-address` command) and then commit your changes.
PAN-25101 (39623)	If you add a Decryption policy rule that instructs the firewall to block SSL traffic that was not previously being blocked, the firewall continues to forward the traffic that is not, yet, decrypted. **Workaround**: Use the `debug dataplane reset ssl-decrypt exclude-cache` command to clear the SSL decrypt exclude cache.
PAN-25046 (39543)	SSH host keys used for SCP log export are stored in the known hosts file on the firewall. In an HA configuration, the SCP log export configuration is synchronized with the peer device, but the known host file is not synchronized. When a failover occurs, the SCP log export fails. **Workaround**: Log in to each peer in HA and **Test SCP server connection** to confirm the host key so that SCP log forwarding continues to work after a failover.
PAN-23732 (37751)	When you use Panorama templates to schedule a log export (**Device** > **Scheduled Log Export**) to an SCP server, you must log in to each managed device and **Test SCP server connection** after the template is pushed. The connection is not established until the firewall accepts the host key for the SCP server.
PAN-20656 (33612)	Attempts to reset the master key from the web interface (**Panorama** > **Master Key and Diagnostics**) or the CLI on Panorama will fail. However, this should not cause a problem when pushing a configuration from Panorama to a device because it is not necessary for the keys to match.
PAN-20162 (32908)	If a client PC uses RDP to connect to a server running remote desktop services and the user logs in to the remote server with a different username, when the User-ID agent queries the Active Directory server to gather user to IP mapping from the security logs, the second username will be retrieved. For example, if UserA logs in to a client PC and then logs in to the remote server using the username for UserB, the security log on the Active Directory server will record UserA, but will then be updated with UserB. The username UserB is then picked up by the User-ID agent for the user to IP mapping information, which is not the intended user mapping.

PAN-OS 7.1.10 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.10 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Starting with PAN-OS 7.1.5, 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-77595	Fixed an issue where PA-7000 Series and PA-5200 Series firewalls forwarded a SIP INVITE based on route lookup instead of Policy-Based Forwarding (PBF) policy.
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-76890	Fixed an issue where traffic that included a ZIP file caused the *all_task* process to restart and the firewall dropped packets while waiting for *all_task* to resume.
PAN-76153	Fixed an issue where PA-5000 Series firewalls dropped traffic because predict sessions incorrectly matched Policy Based Forwarding (PBF) policy rules for non-related sessions.
PAN-75881	Fixed an issue where establishing a TCP session, then installing a content update, and then installing an Antivirus or WildFire update caused the firewall to discard the session, use wrong content for the session, or fail to inspect and perform NAT for the session.
PAN-75413	Fixed an issue where DHCP servers did not assign IP addresses to new end users (DHCP clients) because the firewall failed to process and relay DHCP messages between the servers and clients after you configured a firewall interface as a DHCP relay agent.
PAN-75372	Fixed an issue where Panorama dropped all administrative users because the *management-server* process restarted.
PAN-75273 PAN-61682	Fixed an issue where end users either did not see the Captive Portal web form or saw a page displaying raw HTML code after requesting an application through a web proxy because the HTTP body content length exceeded the specified size in the HTTP Header Content-Length.
PAN-75158	Fixed an issue on HA firewalls in a virtual wire deployment with HA preemption enabled where network outages resulted from Layer 2 looping after failover events while the firewalls processed broadcast traffic.
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.

Issue ID	Description
PAN-74548	Fixed an issue where the Export Named Configuration dialog did not let you filter configuration snapshots by **Name**, which prevented you from selecting snapshots beyond the first 500. With this fix, you can now enter a filter string in the **Name** field to display any matching snapshots.
PAN-74403	Fixed an issue on Panorama where the web interface became unresponsive after you selected **Export to CSV** for a custom report, which forced you to log in to the CLI and reboot Panorama or restart the management server.
PAN-74368	Fixed an issue where commits failed due to configuration memory limits on firewalls that had numerous Security policy rules that referenced many address objects. With this fix, the number of address objects that policy rules reference does not affect configuration memory.
PAN-74236	Fixed an issue where numerous non-browser based requests from clients caused the User-ID process (*useridd*) to stop responding, which resulted in too many `pan_errors` disk writes.
PAN-74188	Fixed an issue where conflicting next-hop entries in the egress routing table caused the firewall to incorrectly route traffic that matched Policy-Based Forwarding (PBF) policy rules configured to **Enforce Symmetric Return**.
PAN-74184	Fixed an issue where Panorama failed to properly create NSX service profile zones and was out of sync with VMware Service Managers after you assigned VMware service definitions to template stacks.
PAN-73914	A security-related fix was made to address OpenSSL vulnerabilities (CVE-2017-3731).
PAN-73783	Fixed an issue where cookie-based authentication for the GlobalProtect gateway failed with the error `Invalid user name`.
PAN-73631	Fixed an issue where end users failed on their first attempt to authenticate through Captive Portal when it was configured for certificate-based authentication and their client certificates exceeded 2,000 bytes.
PAN-73553	Fixed an issue where SSL Inbound Decryption failed when the private key was stored on a hardware security module (HSM).
PAN-73502	Fixed an issue where the firewall did not purge expired IP address-to-username mappings, which caused one of the root partitions to run out of free space.
PAN-73497	Fixed an issue on Panorama where the CSV file that you exported for a custom report (**Monitor > Manage Custom Reports**) included all entries instead of the number of entries specified in the **Sort By** drop-down (such as **Top 10**).
PAN-73484	Fixed an issue where the firewall server process (*devsrvr*) restarted during URL updates.
PAN-73359	Fixed an issue where commits failed because an accumulation of delayed ACC summary reports on Panorama and Log Collectors caused a memory leak in the *reportd* process.
PAN-73281	Fixed an issue where the firewall dropped multicast traffic on an egress VLAN interface if the traffic was offloaded.
PAN-73191	Fixed an issue where OSPF adjacency flapping occurred between the firewall and an OSPF peer due to heavy load on the data plane and queued OSPF hello packets.

Issue ID	Description
PAN-73045	Fixed an issue where HA failover and fail-back events terminated sessions that started before the failover.
PAN-72875	Fixed an issue where the severity level of the syslog message `Failed to sync PAN-DB to peer: Peer user failure` was too high. With this fix, the message severity level is now `info` instead of `medium`.
PAN-72871	Fixed an issue where the firewall displayed only part of the **URL Filtering Continue and Override** response page.
PAN-72697	Fixed an issue where, after a DoS attack ended, the firewall continued generating Threat logs and incrementing the session drop counter.
PAN-72433	Fixed an issue where the PA-7050 firewall displayed incorrect information for the packet counts and number of bytes associated with traffic on subinterfaces. With this fix, the firewall now displays the correct information in the `show interface <interface-name>` CLI command output and in other sources of information for subinterfaces (such as SNMP statistics and NetFlow record exports).
PAN-72346	Fixed an issue where the firewall failed to export botnet reports and displayed the error `Missing report job id`.
PAN-71627	Fixed an issue where the firewall failed to authenticate to a SafeNet hardware security module (HSM). With this fix, the firewall supports multiple SafeNet HSM client versions; you can select the version that is compatible with your SafeNet HSM server through the `request hsm client-version` CLI command.
PAN-71544	Fixed an issue where the VM-Series firewall on Microsoft Hyper-V stopped receiving traffic on interfaces in Tap mode because the system clock went backward, which caused the packet processor to stop.
PAN-71484	Fixed an issue where the firewall disrupted SIP traffic by discarding long-lived SIP sessions after a content update.
PAN-71400	Fixed an issue where the DNS Proxy feature did not work because the associated process (*dnsproxy*) stopped running on a firewall that had an address object (**Objects > Address**) with the same FQDN as one of the **Static Entries** in a DNS proxy configuration (**Network > DNS Proxy**).
PAN-71312	Fixed an issue where custom reports did not display results for queries that specified the **Negate** option, **Contains** operator, and a **Value** that included a period (.) character preceding a filename extension.
PAN-71311	Fixed an issue where, after losing the connection to the Windows-based User-ID agent, the firewall generated a System log with the wrong severity level (`informational` instead of `high`) if you configured the User-ID agent with an FQDN instead of an IP address (**Device > User Identification > User-ID Agents**).
PAN-71133	Fixed an issue on where the dataplane rebooted after multiple dataplane processes restarted due to memory corruption.
PAN-70928	Fixed an issue where the GlobalProtect gateway failed to verify the revocation status of a client certificate using Online Certificate Status Protocol (OCSP).
PAN-70731	Fixed an issue where the firewall failed to authenticate to a SafeNet hardware security module (HSM) if the **Administrator Password** (**Device > Setup > HSM**) contained special characters.

Issue ID	Description
PAN-70366	Fixed an issue where SMTP email servers did not receive PDF reports from the firewall because the report emails used bare LF instead of CRLF line separators.
PAN-69951	Fixed an issue where the firewall generated System logs for `dataplane under severe load` events but failed to forward those logs to Panorama.
PAN-69801	Fixed an issue where the primary firewall peer in an HA active/active configuration was in a tentative HA state and did not synchronize session update messages with the secondary peer, which resulted in dropped packets after a session aged out (within 30 seconds).
PAN-69799	Fixed an issue where PA-7050 firewalls did not correctly enforce log retention periods (**Device > Setup > Management**, Logging and Reporting Settings section, **Log Storage** tab, **Max Days** fields).
PAN-69585	Fixed an issue where the URL link included in the email for a SaaS Application Usage report triggered third-party spam filters.
PAN-69235	Fixed an issue where committing a configuration with 4,000 or more Layer 3 subinterfaces caused the dataplane to stop responding.
PAN-68831	Fixed an issue where CSV exports for Unified logs (**Monitor > Logs > Unified**) had no log entries if you limited the effective queries to one log type.
PAN-68808	Fixed an issue on the PA-7050 firewall where the *mprelay* process experienced a memory leak and stopped running, which caused slot failures and HA failover.
PAN-68795	Fixed an issue where the SaaS Application Usage report displayed upload and download bandwidth usage numbers incorrectly in the Data Transfer by Application section.
PAN-68767	Fixed an issue where Panorama could not change the connection Status of an NSX manager (**Panorama > VMware NSX > Service Managers**) from `Unknown` to `Registered` due to a non-existent null value entry in the NSX manager response.
PAN-68763	Fixed an issue where path monitoring failures did not produce enough information for troubleshooting. With this fix, PAN-OS supports additional debug commands and the tech support file (click **Generate Tech Support File** under **Device > Support**) includes additional registry values to troubleshoot path monitoring failures.
PAN-67699	Fixed an issue where enabling cookie authentication on the GlobalProtect portal (**Network > GlobalProtect > Portals**) caused the *sslvpn* process to stop running, which disconnected end users who connected through an SSL VPN.
PAN-67692	Fixed an issue where Panorama only intermittently used the proxy server if you configured it for connecting to VMware NSX service managers.
PAN-67639	Fixed an issue where the firewall did not properly mask the **Auth Password** and **Priv Password** for SNMPv3 server profiles when you viewed configuration changes in a Configuration log.
PAN-67600	Fixed an issue where firewall interfaces configured as DHCP clients renewed DHCP leases at incorrect intervals.
PAN-67412	Fixed an issue on HA firewalls where, when a user accessed applications over a GlobalProtect clientless VPN, the web browser became unresponsive for about 30 seconds after HA failover.

Issue ID	Description
PAN-66997	Fixed an issue on PA-7000 Series, PA-5200 Series, and PA-5000 Series firewalls where users who accessed applications over SSL VPN or IPSec tunnels through GlobalProtect experienced one-directional traffic.
PAN-66873	Fixed an issue where PAN-OS deleted critical content files when the management plane ran out of memory, which caused commit failures until you updated or reinstalled the content.
PAN-66215	Fixed an issue where the Panorama management server became unresponsive and inaccessible through SSH or HTTPS for several hours.
PAN-65918	Fixed an issue on the Panorama virtual appliance where the third-party backup software BackupExec failed to back up a quiesced snapshot of Panorama. With this fix, the VMware Tools bundled with Panorama now supports the quiescing option.
PAN-64884	Fixed an issue where HA firewalls did not synchronize the Layer 2 MAC table; after failover, PAN-OS rebuilt the MAC table on the peer that became active, which caused excessive packet flooding.
PAN-64870	Fixed an issue where a zone with the **Type** set to **Virtual Wire** (**Network > Zones**) dropped all incoming traffic if the zone had a Zone Protection profile with **Strict IP Address Check** selected (**Network > Network Profiles > Zone Protection > Packet Based Attack Protection > IP Drop**).
PAN-64725	Fixed an issue where Panorama lost its connections to firewalls if it collected logs at a high rate and those logs matched a Panorama report that specified fields requiring DNS lookups.
PAN-64639	Fixed an issue where HA firewalls failed to synchronize the PAN-DB URL database.
PAN-63969	Fixed an issue on HA PA-7050 firewalls where the NPC Ethernet interfaces on the passive peer displayed link activity on a neighboring device (such as a switch) to which they connected even though the interfaces were down on the passive peer.
PAN-63612	Fixed an issue where User activity reports on Panorama did not include any entries when there was a space in the Device Group name.
PAN-62937	Fixed an issue where establishing an LDAP connection over a slow or unstable connection caused commits to fail when TLS was enabled. With this fix, if TLS is enabled, the firewall does not attempt to establish LDAP connections when you perform a commit.
PAN-62797	Fixed an issue where the *cdb* process intermittently restarted, which prevented jobs from completing successfully.
PAN-62791	Fixed an issue where the firewall could not use the certificates in its certificate store (**Device > Certificate Managment > Certificates > Device Certificates**) after a manual or automatic commit, which caused certificate authentication to fail.
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-62436	Fixed an issue where, after you installed the GlobalProtect agent, it failed to connect with the GlobalProtect portal to download the agent configuration because authentication messages had special characters.
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.

Issue ID	Description
PAN-61644	Fixed an issue where Panorama displayed the error `Invalid term(device-group eq)` when you tried to display the logs for a specific device group.
PAN-61409	Fixed an issue where the firewall failed to connect to an HTTP server using the HTTPS protocol when the CA certificate that validated the firewall certificate was in a specific virtual system instead of the Shared location.
PAN-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-60101	Fixed an issue on the M-500 and M-100 appliances in Panorama mode where emailed custom reports contained no data if you configured a report query that used an **Operator** set to **contains** (**Monitor > Manage Custom Reports**).
PAN-59677	A security-related fix was made to prevent firewall administrators logged in as root from using GNU Wget to access remote servers and write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource (CVE 2016-4971).
PAN-59676	Fixed an issue where firewall administrators with custom roles (Admin Role profiles) could not download content or sofware updates.
PAN-58358	Fixed an issue where CSV exports for Unified logs (**Monitor > Logs > Unified**) displayed information in the wrong columns.
PAN-57553	Fixed an issue where a QoS profile failed to work as expected when applied to a clear text node configured with an Aggregate Ethernet (AE) source interface that included AE subinterfaces.
PAN-56453	Fixed an issue where the Correlation logs that Panorama forwarded with a custom Common Event Format (CEF) were incomplete and incorrectly formatted when sent as syslogs.
PAN-56287	Fixed an issue where the firewall discarded VoIP sessions that had multicast destinations.
PAN-56015	Fixed an issue where the syslog format for Correlation logs differed from the format of other log types, which prevented the firewall from integrating with some third-party syslog feeds.
PAN-55245	Fixed an issue on VM-Series firewalls where application-level gateway (ALG) H.245 traffic failed due to a session prediction endian issue.
PAN-54531	Fixed an issue where the firewall stopped writing new Traffic and Threat logs to storage because the Automated Correlation Engine used disk space in a way that prevented the firewall from purging older logs.
PAN-49821	Fixed an issue where connections to the GlobalProtect portal failed when traffic came from a shared gateway and there was no Security policy rule to allow TCP port 20077 for the GlobalProtect portal IP address. With this fix, you need only allow access to TCP port 443 for the GlobalProtect portal even when traffic is coming from a shared gateway.
PAN-49660	Fixed an issue where several processes stopped on HA firewalls that received HA3 messages but didn't have HA3 interfaces configured.

Issue ID	Description
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-OS 7.1.9 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.9 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Starting with PAN-OS 7.1.5, 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
WF500-3605	Fixed an issue where the WF-500 appliance created too many logs when generating PDF reports.
PAN-76265	Fixed an issue where the firewall failed to retrieve user groups from an LDAP server because the server response did not have a page control value.
PAN-75048	Fixed an issue where the firewall used the default route (instead of the next best available route) when the eBGP next hop was unavailable, which resulted in dropped packets. Additionally with this fix, the default time-to-live (TTL) value for a single hop eBGP peer is changed to 1 (instead of 2).
PAN-75005	Fixed an issue where loading a configuration other than running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release removed authentication profiles from GlobalProtect portals and gateways, which caused an auto-commit failure.
PAN-74161	Fixed an issue where firewalls configured in a virtual wire deployment where Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets were dropped.
PAN-74128	Fixed an issue where a session caused the dataplane to restart if the session was active during and after you installed a content update on the firewall and the update contained a decoder change.
PAN-74048	Fixed an issue where numerous NSX dynamic address updates caused Panorama to perform slower and to delay deployment of updates to firewalls. With this fix, you can use the `request partner vmware-service-manager dau-updater-time-interval time-interval <time_interval_in_seconds>` CLI command to set the interval at which Panorama processes the NSX dynamic updates.
PAN-72779	Fixed an issue where the Panorama management server restarted after you installed the latest content database.
PAN-72769	A security-related fix was made to prevent brute-force attacks on the GlobalProtect external interface (CVE-2017-7945).
PAN-72350	Fixed an issue where high-volume SSL traffic intermittently added latency to SSL sessions.
PAN-71530	Fixed an issue where LDAP authentication failed intermittently when the firewall tried to connect to the LDAP server through a service route or after HA failover.
PAN-71455	Fixed an issue where users could not access a secure website if the certificate authority that signed the web server certificate also signed multiple certificates with the same subject name in the Default Trusted Certificate Authorities list on the firewall.

Issue ID	Description
PAN-71319	Updated PAN-OS to address NTP issues (CVE-2016-7433).
PAN-71284	Fixed an issue where Panorama failed to deploy BrightCloud URL filtering database updates to firewalls.
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-71004	Fixed an issue where, when the firewall killed a process (*l3svc*), the process produced child processes that continued running. With this fix, the firewall cleans up the child processes before respawning the l3svc process.
PAN-70620	Fixed an issue where an uninitialized general-purpose I/O (GPIO) controller driver caused the firewall to become unresponsive and require a reboot.
PAN-70541	A security-related fix was made to address an information disclosure issue that was caused by a firewall that did not properly validate certain permissions when administrators accessed the web interface over the management (MGT) interface (CVE-2017-7644).
PAN-70483	Fixed an issue on M-Series appliances in Panorama mode where Security policy rules did not display shared service groups in the service drop-down on the **Service/URL Category** tab if the drop-down had 5,000 or more entries.
PAN-70436	A security-related fix was made to prevent tampering with files that are exported from the firewall web interface (CVE-2017-7217).
PAN-70434	A security-related fix was made to prevent inappropriate disclosure of information through the firewall web interface (CVE-2017-721).
PAN-70426	A security-related fix was made to prevent firewall administrators from performing actions through the web interface that require higher privileges than their administrator roles allow (CVE-2017-7218).
PAN-70345	Fixed an issue where the M-Series appliances did not forward logs to a syslog server over TCP ports.
PAN-70323	Fixed an issue where firewalls running in FIPS-CC mode did not allow import of SHA-1 CA certificates even when the private key was not included; instead, firewalls displayed the following error: `Import of <cert name> failed. Unsupported digest or keys used in FIPS-CC mode`.
PAN-69882	Fixed an issue where firewalls that had multiple virtual systems and that were deployed in an HA active/active configuration dropped TCP sessions.
PAN-69622	Fixed an issue where the firewall did not properly close a session after receiving a reset (RST) message from the server when the SYN Cookies action was triggered.
PAN-68934	Fixed an issue where the SNMP object panSessionActiveSslProxyUtilization contained inaccurate data.
PAN-68873	Fixed an issue where customizing the block duration for threat ID 40015 in a Vulnerability Protection profile did not adhere to the defined block interval. For example, if you set the **Number of Hits** (SSH hello messages) to `3` and **per seconds** to `60`, after three consecutive SSH hello messages from the client, the firewall failed to block the client for the full 60 seconds.
PAN-68520	Fixed an issue where having multiple IPSec IKE gateways configured to the same peer IP address caused VPN tunnels to flap.

Issue ID	Description
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-68210	Fixed an issue where administrators with custom roles could not use the firewall CLI to change the HA state or initiate HA synchronization for the firewall.
PAN-68185	Fixed an issue where the 7.1 SNMP traps MIB file (PAN-TRAPS.my) had an incorrect description for the panHostname attribute.

PAN-67629	Fixed an issue where existing users were removed from user-group mappings when the Active Directory (AD) did not return an LDAP Page Control in response to an LDAP refresh, which resulted in the following User-ID (*useridd*) logs:
	`debug: pan_ldap_search(pan_ldap.c:602): ldap_parse_result error code: 4`
	`Error: pan_ldap_search(pan_ldap.c:637): Page Control NOT found`

PAN-67599	In PAN-OS 7.0 and 7.1 releases, a restriction was added to prevent an administrator from configuring OSPF router ID 0.0.0.0. This restriction is removed in PAN-OS 7.1.9.
PAN-67503	Fixed an issue where the firewall automatically rebooted when you ran a Correlated Events query with more than 15 OR operators.
PAN-67029	Fixed an issue where the firewall stopped forwarding logs to external services (such as a syslog server) after the firewall management server restarted unexpectedly.
PAN-66610	Fixed an issue where memory usage errors occurred if the PAN-OS integrated User-ID agent had numerous servers to monitor for login events. With this fix, the User-ID agent queries five servers at a time to prevent the firewall from exhausting memory.
PAN-66399	Fixed an issue where the active firewall in an HA active/passive configuration did not synchronize GlobalProtect certificates with the passive firewall, which caused a commit failure on the passive firewall.
PAN-66104	Fixed an issue where the firewall displayed shared response pages instead of the custom response pages (Captive Portal, URL continue, and URL override) that were configured for specific virtual systems.
PAN-65969	Fixed an issue on PA-7000 Series firewalls where the Switch Management Card (SMC) restarted due to false positive conditions (ATA errors) detected during a disk check.
PAN-65939	Fixed an issue where you could not download WildFire private cloud updates because the firewall checked for the updates using a proxy server even when you configured the firewall not to **Use Proxy Settings for Private Cloud** (**Device > Setup > WildFire**).
PAN-65669	Fixed an issue where the firewall did not apply a VLAN tag to BFD traffic on a VLAN subinterface.
PAN-64436	Fixed an issue on PA-7000 Series firewalls where creation of IGMP sessions failed because they were stuck in an OPENING state or the wrong state.
PAN-64317	Fixed an issue where IPv6 neighbor discovery failed intermittently due to a corrupted neighbor table.
PAN-63856	Fixed an issue where memory issues caused User-ID processes to restart when multiple firewalls redistributed a large number of IP address-to-username mappings.
PAN-63641	Fixed an issue where the firewall failed to establish connections from some virtual systems to Windows-based User-ID agents and Terminal Services agents.

Issue ID	Description
PAN-63520	Fixed an issue where the firewall used the wrong source zone when logging virtual system-to-virtual system sessions.
PAN-63013	Fixed an issue where a commit validation error displayed when Panorama running a PAN-OS 7.1 or later release pushed a template configuration with a modified WildFire File Size Limits setting (**Device > Setup > WildFire**) to a firewall running a PAN-OS 7.1 or earlier release.
PAN-62622	Fixed an issue where Traffic logs indicated a session was decrypted even though it matched a Decryption policy rule that specifies no decryption and even though no decryption occurred.
PAN-62338	Fixed an issue where the firewall performed NAT translation incorrectly on the passive IP address in data packets when sending passive FTP connections over a proxy tunnel.
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-61439	Fixed an issue where Panorama failed to deploy content updates to Log Collectors when you used the **Install From File** option.
PAN-61300	Fixed an issue where removing and adding a large number of Security policy rules caused Traffic logs to lose their rule name field, which resulted in a commit failure.
PAN-61252	Fixed an issue on firewalls in an HA active/active configuration where the floating IP address was not active on the secondary firewall after the link went down on the primary firewall.
PAN-60333	Fixed an issue where the firewall deployed in an HA active/active configuration with asymmetric routing dropped packets in TCP, ICMP, and UDP traffic.
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 7.1.9 or later release does not cause commit failures related to these settings.
PAN-59542	Fixed an issue on firewalls with multiple virtual systems where the web interface displayed the **Trusted Root CA** option as disabled in certificates for which the option was actually enabled.
PAN-59275	Fixed an issue where processing Oracle application traffic caused the firewall to reboot.
PAN-58382	Fixed an issue where users were matched to the incorrect security policies.
PAN-58212	Fixed an issue where the dataplane restarted unexpectedly when firewalls deployed in an HA configuration missed heartbeats.
PAN-57888	Fixed an issue where the App Scope Traffic Map did not display the correct location of Samoa.
PAN-57529	Fixed an issue where the firewall acted as a DHCP relay and no wireless devices on a VLAN received a DHCP address (all other devices on the VLAN did receive a DHCP address). With this fix, all devices on a VLAN receive a DHCP address when the firewall acts as a DHCP relay.
PAN-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-57440	Fixed an issue where OSPFv3 link-state updates were sent with the incorrect OSPF checksum when the OSPF packet needed to advertise more link-state advertisements (LSAs) than fit into a 1,500-byte packet. With this fix, the firewall sends the correct OSPF checksum to neighboring switches and routers even when the number of LSAs doesn't fit into a 1,500-byte packet.
PAN-57349	Fixed an issue where numerous SSL sessions exhausted the memory pool that the firewall required to insert new certificates in its certificate cache.
PAN-57155	Fixed an issue where custom reports did not display a value for Day Received when running the report on demand (**Run Now**) while the web interface language was set to Japanese. (This was not an issue when exporting the report as a PDF, CSV, or XML file.)
PAN-55536	Fixed an issue where commit failures caused by the firewall commit queue being full did not display the correct error message.
PAN-55048	Fixed an issue where the firewall did not forward logs in the syslog format that you selected.
PAN-52739	Fixed an issue where virtual system administrators saw commit warnings for virtual systems that were outside the scope of their administrative role privileges.
PAN-49764	Fixed an issue where SNMP traps that the firewall generated did not include its system name or hostname.

PAN-OS 7.1.8 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.8 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Starting with PAN-OS 7.1.5, 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-73699	Fixed an issue where UDP IPv6 fragmented packets were dropped due to an incorrect defrag packet attached to the session bind nack message.
PAN-73291	Fixed an issue where authentication failed for client certificates signed by a CA certificate that was not listed first in the Certificate Profile configured with client certificate authentication for GlobalProtect portals and gateways.
PAN-72952	Improved file-type identification for Office Open XML (OOXML) files, which improves the ability for WildFire to accurately classify OOXML files as benign or malicious.
PAN-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-71892	Fixed an issue where an LDAP profile did not use the configured port; the profile used the default port, instead.
PAN-71829	Fixed an issue on PA-5000 Series firewalls where the dataplane restarted due to specific changes related to certificates or SSL profiles in a GlobalProtect configuration—specifically, configuring a new gateway, changing a certificate linked to GlobalProtect, or changing the minimum or maximum version of the TLS profile linked to GlobalProtect.
PAN-71556	Fixed an issue where MAC address table entries with a time-to-live (TTL) value of 0 were not removed as expected, which caused the table to continually increase in size.
PAN-71384	Fixed an issue with the passive firewall in a high availability (HA) configuration that had LACP pre-negotiation enabled where the firewall stopped correctly processing LACP BPDU packets through an interface that had previously physically flapped.
PAN-71215	Fixed an issue where deactivating a VM-Series firewall from Panorama failed and caused the firewall to become unreachable when the **Verify Update Server Identity** setting was enabled in Panorama (**Panorama > Setup > Services > Verify Update Server Identity**) but disabled on the firewall.
PAN-70969	Fixed an issue on a virtual wire where, if you enabled Link State Pass Through (**Network > Virtual Wires**), there were significant delays in link-state propagation or even instances where an interface stayed down permanently even when ports were re-enabled on the neighbor device.

Issue ID	Description
PAN-70923	Fixed an issue where the User-ID process (*userid*) stopped responding when the firewall was having connectivity issues with one of the LDAP servers.
PAN-70428	A security-related fix was made to prevent inappropriate information disclosure to authenticated users (CVE-2017-5583 / PAN-SA-2017-0005).
PAN-70371	Fixed an issue where RADIUS challenge-based authentication failed when user input included uppercase characters.
PAN-69906	Fixed an issue where SNMP packets caused a decoder loop that resulted in high dataplane CPU usage.
PAN-69479	Fixed an issue where renaming a template broke the configuration for any NSX service profile zones within that template.
PAN-69340	Fixed an issue where the capacity license was not applied when you used a license authorization code (capacity license or a bundle) to bootstrap a VM-Series firewall because the firewall did not reboot after the license was applied.
PAN-69194	Fixed an issue where performing a device group commit from a Panorama server running version 7.1 to managed firewalls running PAN-OS 6.1 failed to commit when the custom spyware profile action was set to **Drop**. With this fix, Panorama translates the action from **Drop** to **Drop packets** for firewalls running PAN-OS 6.1, which allows the device group commit to succeed.
PAN-68766	Fixed an issue where navigating to the IPSec tunnel configuration in a Panorama template caused the Panorama management web interface to stop responding and displayed a `502 Bad Gateway` error.
PAN-68489	Fixed an issue where the management interface configured for DHCP caused FQDN resolution to fail.
PAN-68074	A security-related fix was made to address CVE-2016-5195 (PAN-SA-2017-0003).
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 displays a warning when you commit configuration changes.
PAN-68034	The `netstat` CLI command was removed in the 7.1 release for Panorama, Panorama log collector, and WildFire. With this fix, the `netstat` command is reintroduced.
PAN-67944	Fixed an issue where a process (*all_pktproc*) stopped responding because a race condition occurred when closing sessions.
PAN-67090	Fixed an issue where the web interface displayed an obsolete flag for the nation of Myanmar.
PAN-67086	Fixed an issue on PA-7000 Series firewalls where the PA-7000-20GQXM-NPC and PA-7000-20GQ-NPC cards could not achieve more than 16Gbps throughput for non-offloaded traffic. With this fix, the cards can reach the maximum specified throughput of 20Gbps.
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).

Issue ID	Description
PAN-66688	Fixed an issue with memory leaks associated with the *routed* process when allocated memory was not released when no longer needed.
PAN-66436	Fixed an issue where a role-based Panorama administrator could not perform a configuration audit after context-switching to a firewall.
PAN-64889	Fixed an issue on Panorama where attempting to configure dynamic IP objects using the XML API failed, preventing the configuration from being pushed to the managed firewalls.
PAN-64711	Fixed an issue where the predict session incorrectly used the policies of the parent session.
PAN-64638	Fixed an issue where the firewall failed to send a RADIUS access request after changing the IP address of the management interface.
PAN-64588	Fixed an issue where custom reports did not populate correctly when grouped by source country.
PAN-64525	Fixed an issue where User-ID failed to update the allow list for a group name that was larger than 128 bytes.
PAN-64520	Fixed an issue where H.323-based video calls failed when using source NAT (dynamic or static) due to incorrect translation of the *destCallSignalAddress* payload in the H.225 call setup.
PAN-64164	Fixed an issue on Panorama virtual appliances in an HA configuration where, if you enabled log forwarding to syslog, both the active and passive peers sent logs. With this fix, only the active peer sends logs when you enable log forwarding to syslog.
PAN-64081	Fixed an issue on PA-5000 Series firewalls where the dataplane stopped responding due to a race condition during hardware offload.
PAN-63798	Fixed an issue where usernames were displayed in logs and reports when privacy settings in admin role was configured to prevent their display.
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-63054	Fixed an issue on VM-Series firewalls where enabling software QoS resulted in dropped packets under heavy traffic conditions. With this fix, VM-Series firewalls no longer drop packets due to heavy loads with software QoS enabled and software QoS performance in general is improved for all Palo Alto Networks firewalls.
PAN-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-62319	Fixed an issue where multicast entries were pointing to the wrong rendezvous point (RP) IP address because a recycled interface ID allocated for PIM register encapsulation retained an old tunnel interface that pointed to the wrong RP.
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-62057	Fixed an issue where the GlobalProtect agent failed to authenticate using a client certificate that had a signature algorithm that was not SHA1/SHA256. With this fix, the firewall provides support for the SHA384 signature algorithm for client-based authentication.
PAN-62038	Fixed an issue where configurations committed from Panorama stalled at 99% and failed to complete.
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-61304	Fixed an issue where certain Access Domain users (such as vsys administrators) were not able to log in to the web interface on the firewall; instead, they received the following error: `Could not find role profile in running config.`
PAN-60797	Fixed an issue where read-only superusers were able to view threat packet captures (pcaps) on the firewall but received an error ("File not found") when they attempted to export certain types of pcap files (threat, threat extpcap, app, and filtering).
PAN-60662	Fixed an issue on devices where commits failed due to issues with a process (*authd*).
PAN-60630	Fixed an issue where the server-to-client (s2c) flow for RTP predicted sessions were not correctly matching a policy-based forwarding (PBF) rule.
PAN-60591	Fixed an issue where a custom role administrator with commit privileges could not commit configurations using the XML API.
PAN-60402	Fixed an issue where renaming an address object caused the commit to a Device Group to fail.
PAN-59204	Fixed an issue where the firewall did not create an IPSec NAT-T session after a tunnel re-key until it originated a tunnel keep-alive. When this issue occurred, the firewall dropped NAT-T packets.
PAN-58664	Fixed an issue where GlobalProtect connections failed due to a memory leak in a management-plane process (*sslvpn*) that was followed by a process restart with the error `virtual memory limit exceeded.`
PAN-58496	Fixed an issue where custom reports using threat summary were not populated.
PAN-58411	Fixed an issue where PA-7000 Series firewalls were sending report requests even when the `debug skip-condor reports` CLI command was set to `no`.
PAN-57434	Fixed an issue where the firewall reset connections instead of sending an SMTP 5.4.1 error message when SMTP traffic was blocked after detecting a vulnerability signature. With this fix, the firewall sends an SMTP 5.4.1 error message when SMTP traffic is blocked due to a vulnerability signature.
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 up time (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.

Issue ID	Description
PAN-56700	Fixed an issue where the SNMP OID `ifHCOutOctets` did not contain the expected data.
PAN-56684	Fixed an issue where DNS proxy static entries stopped working when there were duplicate entries in the configuration.
PAN-56531	Fixed an issue where you could not select a configured decrypt interface (it did not display) in the **Decrypt Mirror** drop-down (**Device Groups > Objects > Decryption Profile**) when the firewall or appliance was part of a template stack but not a template.
PAN-55035	Fixed an issue where CSV exports of system logs from the web interface did not enclose strings containing commas in quotes, which broke the formatting of the entries. With this fix, strings containing commas are enclosed in double quotes.

PAN-OS 7.1.7 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.7 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Starting with PAN-OS 7.1.5, 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-70349	Fixed an issue where external dynamic list (EDL) objects lost IP addresses and returned 0.0.0.0 when two or more EDL objects used in a security policy referenced the same source URL.
PAN-69546	Fixed an issue on firewalls in an HA active/passive configuration where, if you enabled LACP pre-negotiation, the egress interface on the passive firewall transmitted packets that should have been filtered, which caused packet loss when neighboring switches incorrectly forwarded traffic to the passive firewall. With this fix, the passive firewall correctly filters egress traffic.
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-68487	Fixed an issue where the web interface displayed 24 ports instead of 14 ports for the PA-7000-20GQXM-NPC network processing card.
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-67079	Fixed an issue in PAN-OS 7.1.6 where SSL sessions were discarded if the server certificate chain size exceeded 23KB.
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-65738	Fixed an issue on firewalls in active/active configuration where a newly created BFD profile disappeared after you performed a commit operation on either of the peers.
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-64626	Fixed an issue where a memory leak occurred on a process (*authd*) after each commit, which caused restarts of another process (*mgmtsrvr*) and affected access to the web interface.
PAN-64435	Fixed an issue on Panorama virtual appliances where a process (*configd*) experienced high memory usage and stopped responding, which caused commits to fail.

Issue ID	Description
PAN-64321	Fixed an issue where Panorama did not update the names of log forwarding profiles and zone protection profiles in a template stack after renaming, which caused failures when pushing the configuration to devices.
PAN-64177	Fixed an issue where the CLI command `test custom-url` did not return the correct custom category.
PAN-63901	Fixed an issue where TCP sequence numbering shifted when the firewall performed a decrypted session tear down in the case of a fatal alert.
PAN-63796	Fixed an issue on PA-7000 Series firewalls where internal looping of tunnel creation packets caused high dataplane CPU usage.
PAN-63038	Fixed an issue on Panorama where traffic logs retrieved by XML API query displayed IP addresses with subnet notation instead of full IP addresses. This issue occurred when the administrator using the query had a custom privacy configuration in the web interface that had **Show Full IP Addresses** disabled.
PAN-63021	Fixed an issue where policy-based forwarding (PBF) symmetric return traffic enforcement failed intermittently because return MAC address entries aged-out prematurely. With this fix, the firewall enforces symmetric return even when PBF return MAC entries age out.
PAN-62944	Fixed an issue where the management server process stopped responding when a **Commit All** job was initiated from Panorama, which prevented managed devices from reporting the commit job status back to Panorama. As a result, the commit job appeared stalled in Panorama even after commits were successfully completed on the managed devices.
PAN-62212	Fixed an issue where the Global Find window was grayed-out and non-functional if you accessed it from the **Browse** link when configuring an address object in a security policy.
PAN-62050	Fixed an issue where a User-ID redistribution loop caused high management plane CPU usage. This issue occurred when the User-ID redistribution configuration included three or more firewalls, and the firewall encountered the same IP address and timestamp for different users.
PAN-61742	Fixed an issue where the firewall incorrectly identified BGP traffic as traceroute traffic, causing the wrong policy to be applied to the traffic.
PAN-61643	Fixed an issue where locally created certificates had duplicate serial numbers because the firewall did not check the serial numbers of existing certificates signed by the same CA when generating new certificates.
PAN-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.
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.

Issue ID	Description
PAN-59870	Fixed an issue where purged software packages appeared in the list of uploaded software packages. With this fix, the software list will no longer display purged software packages.
PAN-59669	Fixed an issue where Online Certificate Status Protocol (OCSP) verification failed when using non-CA certificates. With this fix, you can configure a non-CA certificate as an OCSP Verify certificate (**Device > Certificate Management > Certificates Profile > Add**). Note that if you use a non-CA certificate and then downgrade to a PAN-OS release that does not include this fix, auto-commits will work, but manual commits will fail.
PAN-58744	Fixed an issue where IPSec VPN tunnels failed to establish if you used dynamic VPNs and mixed IKEv1 and IKEv2 on the static device.
PAN-58582	Fixed an issue where the hostname obtained from a Panorama template for a firewall reverted to the default hostname. This issue occurred after the management server process on the firewall (*mgmtsrvr*) restarted following an event such as a PAN-OS update or firewall restart.
PAN-58520	Fixed an issue where PDF exports of custom reports generated using **Run Now** did not display hostnames obtained from reverse DNS lookup.
PAN-57874	Fixed an issue where IPSec tunnels flapped randomly because a race condition between two processes (*mprelay* and *pan_task*) caused duplicate tunnel monitoring ICMP packets with the same sequence numbers to be sent, which disrupted IPSec tunnel state.
PAN-57360	Fixed an issue where the management server process (*mgmtsrvr*) had an out-of-memory condition and restarted, causing a loss of uncommitted changes.
PAN-57181	Fixed an issue on Panorama in an HA configuration where synchronization failed after a commit with the message, `Committing mgt settings failed. Could not read merged running config from file`. This issue occurred when WildFire updates created a race condition with HA synchronization.
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-56189	Fixed an issue where a custom role administrator who had threat log viewing privileges disabled could view threat logs in the Unified log view.
PAN-55747	Fixed an issue where websites failed to load properly if you enabled SSL decryption. This issue occurred due to an error in the handling of URL block pages and captive portal redirects.

PAN-OS 7.1.6 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.6 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Starting with PAN-OS 7.1.5, 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-68586	Fixed an issue where adding, removing, or modifying the Import/Export rules in a BGP configuration caused BFD and BGP neighbor state to flap.
PAN-67730	Fixed an issue where a process (*l3svc*) stopped responding multiple times with the message `l3scv: Exited 4 times, waiting xxxx seconds to retry`. With this fix, the failing process (*l3svc*) will no longer exit inadvertently.
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-66991	Fixed an issue where, if the firewall received an empty SCEP authentication cookie from a GlobalProtect agent, a process (*ssl-mgr*) on the firewall restarted. With this fix, the process does not restart when it receives an empty authentication cookie (the cookies are transparent to the user and cannot be configured).
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 between firewalls and 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 these issues.
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-65996	Fixed an issue where, if a connection to the LDAP server failed, the authentication process (*authd*) stopped processing GlobalProtect user authentication requests, and, eventually, all subsequent successful authentication requests were dropped because the retry-interval flag was not set correctly. With this fix, authentication functions normally after the retry interval.
PAN-64796	Fixed an issue where a process (*logrcvr*) consumed more memory than expected when a WildFire update occurred if you enabled correlation objects (**Monitor > Automated Correlation Engine > Correlation Objects**).
PAN-64727	Fixed an issue where the firewall changed the sequence numbers of forwarded TCP keep-alive packets.

Issue ID	Description
PAN-64582	Fixed an issue where a memory leak prevented secure websites from loading correctly if the URL filtering configuration blocked some objects on the page and a decryption profile rule applied “No Decrypt” to the website.”
PAN-64368	Fixed an issue on PA-7000 Series firewalls where, if you applied a Quality of Service (QoS) profile to an Aggregated Ethernet (AE) interface, the QoS statistics reported a maximum egress for the AE interface that differed 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 the AE interface.
PAN-64361	Fixed an issue where the DNS proxy failed for DNS traffic that used TCP as the transportation protocol and DNS servers contained DNS records with a very large number of entries (more than 100).
PAN-64360	Fixed an issue where the firewall failed to populate the email sender, recipient, and subject information for WildFire reports.
PAN-64263	Fixed an issue where forward-proxy decryption failed if the server certificate record size exceeded 16KB.
PAN-63928	When a limited-role user accessed the web interface on the firewall and made changes from the Panorama context, the firewall applied an automated commit lock that could not be removed from that user.
PAN-63818	Fixed an issue on Panorama where, after you added a zone to a template, the zone failed to show up in the drop-down when choosing the source in a security policy.
PAN-63800	Fixed an issue where, if you enabled decryption on the firewall with a decryption profile that did not use Diffie-Hellman (DHE) and Elliptic Curve Diffie-Hellman (ECDHE) ciphers, the firewall sent an elliptic curve extension in the Client Hello, which caused the server to decline the connection.
PAN-63315	Fixed an issue where the custom response page for URL overrides failed to display.
PAN-63142	Fixed an issue where the dataplane restarted when processing IPv6 traffic that matched a predict session.
PAN-63080	Fixed an issue where a process (*websrvr*) stopped responding, which caused the captive portal to not function. This issue occurred when you had a custom response page that used a large binary object.
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 an LDAP query that terminated before completion resulted in a memory corruption.
PAN-62385	Fixed an issue where, if the firewall lost connectivity with an LDAP server or if you applied an invalid query filter, and the disruption 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, but does not delete existing user-group mappings.
PAN-62261	Fixed an issue where the DNS proxy failed for DNS traffic that used TCP as the transportation protocol.
PAN-62188	Fixed an issue where, if you configured a large number of FQDN objects, the firewall required multiple commits to refresh the objects.

Issue ID	Description
PAN-61554	Fixed an issue where a memory leak in a process (*authd*) caused all authentications to the firewall to fail.
PAN-61547	Fixed an issue where a process (*snmpd*) had a memory leak that caused frequent SNMP restarts.
PAN-61543	Fixed an issue where, after you committed a push from the Panorama web interface to a device, the commit job appeared to stall at 0% complete even the Panorama successfully pushed the configuration.
PAN-61468	A security-related fix was made to address CVE-2016-6210 (PAN-SA-2016-0036).
PAN-61436	Fixed an issue where SSL Forward Proxy decryption failed with the error `Unsupported Version` if the server returned a very large certificate. With this fix, decryption succeeds even for very large certificates.
PAN-61428	Fixed an issue where the firewall allowed a GlobalProtect client to connect without validating the client certificate.
PAN-61104	A security-related fix was made to address a local privilege escalation issue (PAN-SA-2016-0034).
PAN-60933	Fixed an issue on firewalls in an HA active/passive configuration where, if you enabled LACP prenegotiation, the passive firewall intermittently forwarded traffic.
PAN-60893	Fixed an issue where the API command `show object registered-ip all option count` failed to produce the correct output where there were more than 500 registered entries. When this issue occurred, the command returned a file location for a file that listed the IP addresses instead of returning a count. With this fix, the API command functions correctly where there are more than 500 registered entries and returns the same output as the equivalent CLI command.
PAN-60390	Fixed an issue on Panorama where, if a RADIUS user logged in and tried to commit a configuration change, the commit window appeared and then disappeared before it could be read by the user.
PAN-59715	Fixed an issue where the GlobalProtect agent disconnected from the GlobalProtect gateway under high traffic loads. This issue occurred when the connections employed SSL tunnels instead of IPSec tunnels.
PAN-59532	Fixed an issue where, if you imported a device configuration into Panorama, and then pushed the configuration to a firewall, the commit failed with the error `region unexpected here`.
PAN-59411	Fixed an issue where a process (*logrcvr*) stopped responding, which caused commit and OSPF adjacency failures. With this fix, the process uses the correct buffer size to prevent the fault.
PAN-58906	Fixed an issue where, if you deselected the **Log at Session End** option, the log still generated entries for security policies with a configured URL category and an action other than **Allow**. With this fix, the firewall does not generate log entries if the option is deselected.
PAN-58822	Fixed an issue where the firewall blocked a static route configuration for the IPv4 destination 0.0.0.0/1. With this fix, the firewall allows configuration of static route entries in the range of 0.0.0.0/[0-7].

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-58618	Fixed an issue where the firewall dataplane restarted if you enabled data leak prevention (DLP).
PAN-58602	Fixed an issue where a Panorama template commit to a firewall failed with the error `LDAP is missing 'ssl'`. This issue occurred when the firewall operated in CCEAL4 mode.
PAN-58589	Fixed an issue where the dataplane restarted when an out-of-memory condition occurred on a process (*pan_comm*).
PAN-58526	Fixed an issue where Kerberos authentication to the Captive Portal was unsuccessful if the Kerberos token was larger than 8,000 bytes.
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-58508	Fixed an issue where the firewall tried to create IP address-to-username mappings for IP addresses in the zone exclude list if the addresses were configured as address objects.
PAN-58413	Fixed an issue on firewalls and Panorama where, if you attempted to manually upload a software image that was larger than 1GB from the web interface, the upload failed with the error `Upload file size exceeded system limit`. With this fix, the firewall and Panorama size limit on software image uploads is increased.
PAN-58410	Fixed an issue on VM-Series firewalls in an HA configuration where an interface on the active firewall displayed its status as `ukn/ukn/down(autoneg)` after a failover occurred.
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-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 or in custom reports.
PAN-57785	Fixed an issue where the CLI commands `show wildfire status` and `test wildfire tor` returned Tor status errors. With this fix, the CLI commands only return Tor status errors in the case of an actual communication error.
PAN-57593	Fixed an issue where a decryption policy stopped decrypting SSL traffic if you enabled **Wait for URL** on SSL decryption.
PAN-57514	Fixed an issue where correlation logs forwarded from Panorama to an external syslog server contained a dash (`-`) instead of the Panorama hostname.
PAN-57358	Fixed an issue on Panorama where, if you tried to import a device state bundle in the device context (**Device > Operation > Import**), the import failed with the error message `Error in copying file`. With this fix, device state import works as expected.

Issue ID	Description
PAN-57145	Fixed an issue where, if the firewall performed IP and port NAT in the path of a GlobalProtect 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, which prevents 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-56969	Fixed an issue where the firewall did not record X-Forwarded-For (XFF), User-Agent, or Referral HTTP headers in the URL log if the traffic was blocked or reset by a security profile even when HTTP header logging was enabled and the traffic contained those fields. With this fix, the firewall correctly logs the HTTP Headers.
PAN-56831	Fixed an issue on PA-7000 Series firewalls where, if the firewall processed UDP packets using an inter-vsys configuration, the packets looped repeatedly from one dataplane to another and increased dataplane CPU consumption to nearly 100%. With this fix, the firewall does not create a loop condition and processes the packets correctly.
PAN-56775	Fixed an issue where a firewall configured to perform a monthly update of the external dynamic list (EDL) initiated an EDL refresh job every second.
PAN-56438	Fixed an issue 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-56257	Fixed an issue where reverse proxy key log entries did not contain Common Name (CN) information when a certificate mismatch occurred.
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-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-55474	Fixed an issue on firewalls in an HA active/passive configuration where, if you configured the path monitor timers with an aggressive value, the firewalls entered an unstable state with one node eventually becoming non-functional.
PAN-55344	Fixed an issue where the web interface limited the high availability (HA) active/active IPv6 virtual address field to 31 characters.
PAN-55237	A security-related fix was made to address an XPath injection vulnerability in the web interface (PAN-SA-2016-0037).
PAN-55196	Fixed an issue where the firewall did not resolve the IPv4 addresses of configured FQDN objects if you disabled firewalling for IPv6 addresses and you configured FQDN objects with both IPv4 and IPv6 addresses.
PAN-55190	Fixed an issue where a firewall 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.

Issue ID	Description
PAN-54492	Fixed an issue on firewalls and Panorama where SaaS reporting failed and a process (*saas_report_wra*) did not exit properly after the reporting failure.
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-53860	Fixed an issue where SSL decryption did not occur if the SSL handshake was very large.
PAN-52138	Fixed an issue on firewalls with destination NAT enabled where video calls from outside the network failed because the firewall did not properly translate connect packets.
PAN-51703	Fixed an issue where a firewall process (*all_pktproc*) stopped responding after upgrading a firewall to a PAN-OS 7.1 release,
PAN-39257	Fixed an issue where you could forge the URL filtering `continue` action by modifying the User-ID (`uid`) parameter in the URL presented by the firewall. This issue occurred in a limited context where a malicious second user clicked on the `Continue` page alert on behalf of the actual user.

PAN-OS 7.1.5 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.5 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Starting with PAN-OS 7.1.5, 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-63171	Fixed an issue where, when using the GlobalProtect agent on a Mac OS X endpoint, the connection from the agent to the GlobalProtect gateway failed and the agent displayed the error `Certificate error. Restart the service?`.
PAN-63080	Fixed an issue where, if you had a custom response page that used a large binary object, a process (*websrvr*) stopped responding, which caused the captive portal to not function.
PAN-62803	Fixed an issue where, if you configured GlobalProtect to use certificate-based authentication, users on Chromebook endpoints received prompts to log on using username and password.
PAN-62773	Fixed an issue on VM-Series firewalls in an HA configuration where synchronization traffic lead to a condition where the firewall stopped responding.
PAN-62589	Fixed an issue on Panorama where a stack configuration was incomplete and failed with the error message `Failed to create configuration for template`, even though the composing templates had configuration entries present.
PAN-62339	Fixed an issue where a process (*websrvr*) restarted repeatedly during captive portal redirects because the redirect URL did not include required vsys and URL arguments.
PAN-61818	Fixed an issue where CPU utilization on the dataplane was higher than expected.
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-61547	Fixed an issue where a process (*snmpd*) had a memory leak that caused frequent SNMP restarts.
PAN-61521	Fixed an issue on Panorama where, if you added a User-ID agent to a template in a template stack, and one of the templates in the stack did not have a User-ID agent specified, you would lose User-ID agents from templates in the stack.
PAN-61146	Fixed an issue where, if you changed or refreshed an FQDN configuration with a large number of IP address entries (more than 32 IPV4 and IPV6 entries) in a single FQDN object, the firewall or Panorama management server stopped responding.
PAN-61046	A security-related fix was made to address a cross-site request forgery issue (PAN-SA-2016-0032).
PAN-60872	Fixed an issue where WildFire falsely identified Microsoft Word files containing macros as suspicious.

Issue ID	Description
PAN-60830	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.
PAN-60828	Fixed an issue where a process (*l3svc*) restarted due to missing too many heartbeats, which caused the Captive Portal to fail to trigger.
PAN-60819	Fixed an issue where the dataplane restarted while processing a chain of tunnel packets.
PAN-60667	Fixed an issue where a process (*devsrvr*) restarted repeatedly due to a problem with the internal URL cache structure.
PAN-60587	Fixed an issue where the firewall did not provide a blocked page response if you accessed a blocked application over HTTPS.
PAN-60568	A security-related change was made to address a version disclosure in GlobalProtect (PAN-SA-2016-0026).
PAN-60444	Fixed an issue where SCEP enrollment failed when parsing CA certificates sent by the Aruba ClearPass server.
PAN-60002	Fixed an issue 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.
PAN-59778	Fixed an issue where, in very rare cases, the firewall forwarded frames to incorrect ports because duplicate MAC address entries were present in the offload processor MAC table. With this fix, the offload processor will not have duplicate MAC address entries in the MAC table.
PAN-59704	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.
PAN-59634	Fixed an issue in WildFire that led to a false negative detection on a malicious file. With this fix, WildFire detects malicious files that launch via powershell.exe.
PAN-59565	Fixed an issue where exported log files did not correctly escape certain characters, such as commas (`,`), backslashes (\\), and equal-to operators (=).
PAN-59470	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.
PAN-59451	Fixed an issue where the captive portal response page did not display the user's IP address as specified by the `<user/>` variable in the HTML code for the page.
PAN-59315	Fixed an issue where a delay occurred on HA failover following a control plane failure on the active firewall.

Issue ID	Description
PAN-59258 98112	Fixed an issue on firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt. However, in PAN-OS 7.1.4, this issue is fixed only for an HA pair where both peers are running a PAN-OS 7.1 release; this issue is not fixed in a configuration where one firewall is running a PAN-OS 7.1 release and the other is running a PAN-OS 7.0 or earlier release.
PAN-58896	Fixed an issue where, if you used the CLI command `request system fqdn show` to display FQDN objects, the firewall displayed extra IP addresses that were not associated with the FQDN.
PAN-58885	Fixed an issue where dataplane CPU usage became excessive.
PAN-58816	Fixed an issue where, if you configured multiple virtual systems (Vsys) with non-consecutive identifying numbers, an SNMP poll of the panVsysActiveSessions OID incorrectly showed zero session values for some virtual systems. With this fix, SNMP polling output is correct and matches the equivalent CLI output of the same data.
PAN-58657	Fixed an issue on PA-7000 Series firewalls where a slot stopped responding due to a memory condition.
PAN-58322	Fixed an issue 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**.
PAN-58086	Fixed an issue 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-57659	A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0031).
PAN-57464	Fixed an issue where end users experienced delays because the firewall sent an RST packet without an ACK flag to the client. This issue occurred when the firewall applied a security policy action of `Reset Client` or `Reset Both`.
PAN-57383	Fixed an issue where SSL decrypted traffic that used an unsupported RSA key size of 16384 caused the dataplane to restart.
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 re-key process.
PAN-57200	Fixed an issue where you could not restart certain firewall processes from the CLI without root access. With this fix, you can now restart these processes (*bfd*, *cryptod*, *dhcpd*, *ikemgr*, *keymgr*, and *pppoed*) using the CLI command `debug software restart process`. See CLI Changes in PAN-OS 7.1 for more information.
PAN-57054	Fixed an issue where, if you redistributed User-ID mapping information and the mapping used a timeout value of `NEVER`, the firewall incorrectly changed the timeout value to 3600.

Issue ID	Description
PAN-56937	Fixed an issue where, if you viewed a configuration diff on the active Panorama server in an HA pair, a process (*configd*) restarted on the passive Panorama server.
PAN-56924	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 where Panorama used a PAN-OS 7.x release and firewalls used a mixture of PAN-OS 6.x and PAN-OS 7.x releases.
PAN-56918	Fixed an issue where firewalls did not recognize malware that had been Base64 encoded in a zipped RTF file. This issue occurred during an SMTP session.
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-56580	Fixed an issue where throughput in an IPSec tunnel was lower than expected. With this fix, the firewall defaults the DSCP field to 0 for ESP packets to improve performance.
PAN-56456	Fixed an issue where, if you implemented an authorization profile for OSPF with MD5 authentication on a firewall configured for FIPS-CC mode, the dataplane restarted.
PAN-56438	Fixed an issue 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-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-55996	Fixed an issue where the dataplane restarted when processing SSL packets with an oversized Layer 2 header.
PAN-55993	Fixed an issue where user authentication based on user groups stopped working after you enabled the multiple virtual systems (multi-vsys) feature.
PAN-55560	Fixed an issue where a memory condition caused the dataplane to restart with the message `Dataplane is down: too many dataplane processes exited`.
PAN-55190	Fixed an issue where the firewall 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, the firewall handles out-of-memory errors correctly, allowing proper resolution of URLs.
PAN-54696	Fixed an issue where incorrect handling of selective-acknowledgment (SACK) packets caused a decrease in download speeds on SSL-decrypted traffic.

Issue ID	Description
PAN-54309	Fixed an issue in Panorama and where the default value of `Save User Credentials` in **Network > GlobalProtect > Portals > GlobalProtect-portal-config > Agent > agent-config > Authentication** was `No` when it should have been `Yes`.
PAN-54196	Fixed an issue where the firewall did not increment the packet identifier of RADIUS Access-Request packets as required by the RFC standard.
PAN-52379	A security-related fix was made to address CVE-2015-5364 and 2015-5366 (PAN-SA-2016-0025).
PAN-52202	Fixed an issue where Panorama, when configured with a log collector, showed logs for a previous date and did not refresh the log display to show the latest logs.
PAN-49329	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.

PAN-OS 7.1.4-h2 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.4-h2 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Issue ID	Description
PAN-60681 99934	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.
97601	Fixed an issue where dataplane CPU usage became excessive.

PAN-OS 7.1.4 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.4 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Issue ID	Description
99996	Fixed an issue where the GlobalProtect agent was unable to retrieve an SCEP-issued user certificate because the firewall sent an invalid response to the agent, which caused the agent to stop responding. With this fix, the firewall sends responses that can be handled by the agent.
PAN-59258 98112	Fixed an issue on firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt. However, in PAN-OS 7.1.4, this issue is fixed only for an HA pair where both peers are running a PAN-OS 7.1 release; this issue is not fixed in a configuration where one firewall is running a PAN-OS 7.1 release and the other is running a PAN-OS 7.0 or earlier release.
98164	Fixed an issue on firewalls where, if you deleted the proxy server configuration for the AutoFocus service, the configuration remained.
97763	Fixed an issue where a PA-200 firewall failed to download a PAN-OS software update due to an incorrect disk space calculation.
97734	Fixed an issue where the GlobalProtect pre-logon VPN failed to establish because the firewall prepended the domain name to pre-logon user.
97689	Fixed an issue where firewalls stopped responding because dynamic IPSec peers sent `X509_SUBJECT` in the Internet Key Exchange (IKE) payload during Phase 1 negotiation.
97625	Fixed an issue on VM-Series firewalls running on Amazon Web Services (AWS) where a process (*devsrvr*) stopped responding after activating the BrightCloud URL filtering license.
97583	Fixed an issue where, with SSL Forward Proxy Decryption enabled, the firewall displayed an expired certificate error page to end users even though the certificate chain was valid because there was an expired certificate on the firewall that was not part of the chain. With this fix, the firewall does not display the misleading error page.
97571	Fixed an issue where reusing previous port information (tcp-reuse) for new sessions caused traffic in those sessions to be dropped.
97549	Fixed an issue on PA-7000 Series firewalls where the system log message `Syslog connection failed to server` appeared repeatedly on the passive firewall of an active/passive pair when the error condition was not present. With this fix, the firewall does not display the log message under incorrect conditions.
97466	Fixed an issue where a TCP reassembly failure for a reused TCP session prevented users from accessing Windows Server 2012 sites and applications.

Issue ID	Description
97424	Fixed an issue where firewalls delayed SSL traffic when unable to resolve the URL category because the Server Certificate Hostname contained a colon character that the firewall interpreted as a delimiter for a port number.
97357	Fixed an issue where a process (*l3svc*) stopped responding while processing captive portal requests that did not have query arguments.
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.
97160	Fixed an issue where a firewall failed to upgrade to a PAN-OS 7.1 release—or where a firewall running a PAN-OS 7.1 release failed to update to a new content release version—and started rebooting repeatedly. This issue occurred when the firewall configuration included an application risk override and the update or upgrade changed that overridden application to a container (`<application>-base`). With this fix, the upgrade or update is successful even if an update or upgrade changes an overridden application to a container.
97113	Fixed an issue where a filter (`url contains`) failed to return results from the URL filtering logs if it contained a generic domain like `com` or `org`. With this fix, filters such as `nytimes.com` and `nytimes` will return equivalent results.
97099	Fixed an issue where, after importing the configuration from a Panorama M-100 appliance to a Panorama M-500 appliance, you could not select the existing security profiles and log-forwarding profiles.
97063	Fixed an issue where User ID group mapping stopped working due to a race condition.
96937	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.
96757	Fixed an issue on Panorama where an administrator lost access after trying to commit a Security policy rule that contained an empty address group.
96679	Fixed an issue where the active-secondary firewall of an HA active/active pair displayed the error message `502 Bad gateway` instead of an expected URL override page to end users.
96422	Fixed an issue where a Panorama administrator with custom rights configuration could not access the commit window because the window flashed and disappeared after the administrator clicked the **Commit** button. With this fix, when an administrator does not have privileges to access a commit function, Panorama displays an error message that indicates access is denied.
96415	Fixed an issue where the firewall failed to pass traffic in strongSwan and Azure IPSec tunnels while using IKEv2 because it did not send a Delete payload during a Phase 2 Child SA re-keying. With this fix, the firewall correctly sends a Delete payload during re-keying if it is the node that initiated the re-keying.
96402	Fixed an issue where a newly active firewall in an HA active/passive pair lost the ability to send TCP SYN messages to its BGP peers, which resulted in dropped traffic.

Issue ID	Description
96184	Fixed an issue where the firewall stopped forwarding logs and discarded logs even when incoming logging rate was low. With this fix, the processing of logs is optimized to improve pre-matching results, and CPU load is reduced to prevent the queue from becoming full and discarding logs.
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.
95978	Fixed an issue where 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.
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.
95846	Fixed an issue where deleting the default administrator account on the VM-Series firewall in AWS caused the firewall to go into maintenance mode. This occurred because the firewall, to reboot successfully, required the SSH key associated with the administrator account (the private key—`ssh-key`—used to provision the firewall in AWS). With this fix, as long as you first create another superuser account on the firewall, you can delete the default administrator account and the firewall will reboot successfully.
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.
95723	Fixed an issue where authentication failed when you used secure encrypted cookies if you configured the GlobalProtect portal or gateway to authenticate using an authentication sequence and then specified a domain\user in the User/User Group settings of the agent configuration.
95622	Security-related fixes were made to address issues identified in the May 3, 2016 OpenSSL security advisory (PAN-SA-2016-0020).
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.
95591	Fixed an issue where management server would crash due to excessive printing of debug messages caused by a large number of FQDN requests.
95568	Fixed an issue where configuration commits on firewalls failed because improper handling of temporary files related to HA sync for registered IP addresses consumed all available space in the target (`pancfg`) disk partition. With this fix the firewall eventually deletes temporary files so they don't accumulate and consume disk space.

Issue ID	Description
95466	Fixed an issue where Panorama displayed a false commit warning that indicated a WildFire scheduled update time overlapped with content updates (Applications, Threats, and Antivirus). With this fix, PAN-OS correctly interprets the WildFire schedule update time and prevents false commit warnings when scheduled update times do not overlap.
95039	Fixed an issue on VM-Series firewalls where traffic processing slowed down for two to three minutes after firewall received a burst of packets on the HA2 data link.
94922	Fixed an issue 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.
94820	Fixed an issue on Panorama where the **Adjust Columns** option in **Panorama** > **Device Groups** did not adjust columns properly and caused fields to disappear from view.
94615	Fixed an issue on PA-7000 Series firewalls where the designated Log Card interface did not transmit a gratuitous ARP upon failover, which caused connectivity issues with neighboring devices.
94582	Fixed an issue where, after you changed the application risk value to a non-default value, the web interface displayed the default value and you could only see the configured value by selecting the application and viewing it manually. With this fix, the firewall displays the configured value in the interface.
94372	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.
94368	Fixed an issue where, if you configured an external dynamic lists file with comments indicated by forward slashes (`//`), the firewall failed to load the file.
94166	Fixed an issue 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.
93921	Fixed an issue where commits on Panorama failed because a process (*cord*) stopped responding.
93909	Fixed an issue where, if the antivirus and anti-spyware definition files for an application were not present, the firewall validated host information profile (HIP) reports with invalid dates.
93540	Fixed an issue where the read-only superuser could not export a threat packet capture (pcap) file from the web interface, which displayed a `File not found` message.
93243	Fixed an issue where a Security policy rule pushed from Panorama could not be cloned locally on the firewall.
92762	Fixed an issue where, regardless of the configured metric, OSPF preferred Type 2 external metrics over Type 1 external metrics.
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.

Issue ID	Description
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.
92527	Fixed an issue where SSL Inbound Inspection caused a packet buffer leak, leading to degraded performance.
92523	Fixed an issue where, for firewalls in an HA active/active configuration, the predict session for an Oracle redirect that 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 predict session for the Oracle redirect transitions to active state to allow for successful Oracle client-to-server communication.
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.
92367	Fixed an issue on Panorama where you could not filter by device group when in the firewall device context.
92106	A security-related fix was made to address multiple NTP vulnerabilities (PAN-SA-2016-0019).
92008	Fixed an issue where, if you used SNMP to check the status of a tunnel interface, the firewall provided incorrect information.
91886	A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0021).
91885	Fixed an issue where the log filter you can create by clicking a value in the Destination Country or Source Country column did not work when you chose a country name because the filter string used the country name instead of the country code.
91767	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**.
91492	Fixed an issue where SSL decryption on firewalls failed when the server presented a certificate chain that did not have the expected extension in the root certificate even though the firewall had the correct root certificate in its default trusted CA store.
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.
91078	Fixed an issue where the `Reject Default Route` configuration did not work for OSPFv3, which resulted in network outages.
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.
90777	Fixed an issue where the firewall failed to make the CLI configuration `set authentication radius-vsa-on client-source-ip` persistent across system restart.

Issue ID	Description
90677	Fixed an issue where the flow management (*flow_mgmt*) process stopped responding, which caused the dataplane to restart.
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.
88696	Fixed an issue where, under certain conditions, a process (*mpreplay*) frequently restarted due to excessive internal messaging.
87032	Fixed an issue where firewalls and appliances running Panorama 7.0 or later releases failed to display or download reports received from firewalls running PAN-OS 6.1 or earlier releases.
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.
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.
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.
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.
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.
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.
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.
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).
84373	Fixed an issue where Panorama generated an error when a WildFire update was installed even though the download and install were successful.

Issue ID	Description
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.
82138	Fixed an issue where WildFire reports were not displayed on the web interface when proxy settings were configured for the management interface.
80628	Fixed an issue where WildFire content updates showed timestamps with future dates.
77822	Fixed an issue where a VM-Series NSX edition firewall sent Dynamic Address Group information only to the primary virtual system (VSYS1) on the integrated physical firewall at the data center perimeter. With this fix, a VM-Series NSX edition firewall configured to Notify Device Group sends Dynamic Address Group updates to all virtual systems on a physical firewall running PAN-OS 7.0.8 or a later PAN-OS 7.0 release.
76197	Fixed an issue where firewall Traffic logs displayed unusually large byte counts for http-proxy and http-video counters due to frequent application shifts between those application-type packets within a single proxy session.

PAN-OS 7.1.3 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.3 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Issue ID	Description
98602	Fixed an issue where the Panorama management server had a memory increase due to syncing of WildFire reports from Panorama to log collectors.
97313	Fixed an issue where the management plane of Panorama M-100 and M-500 appliances stopped responding when renaming objects or Security policy rules 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.
96634	Fixed an issue where a certificate signing request (CSR) using Simple Certificate Enrollment Protocol (SCEP) over SSL failed due to buffer limit (signing over non-SSL worked correctly).
96140	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).
95747	VLAN tag translation is enhanced so that the firewall now preserves the Priority Code Point value (802.1P) in the Layer 2 VLAN tag field when receiving a frame on one VLAN Tag port and then forwarding it to another VLAN Tag port. See Changes to Default Behavior for more information about this enhancement in PAN-OS 7.1.3 and about further enhancements in PAN-OS 7.1.5.
95275	Fixed an issue where a role-based administrator could view unified logs under the **Monitor** tab but could not export these logs.
95133	Fixed an issue where firewall incorrectly applied Policy Based Forwarding (PBF) to sessions created via prediction (such as ftp-data sessions).
95047	Fixed an issue where PAN-OS log integration with AutoFocus did not use proxy server settings.
94930	Fixed an issue where firewall running on a VMware NSX edition firewall had incorrect address-group objects pushed via Panorama updates.
94914	Fixed an issue where a firewall running PAN-OS 7.1 failed to block HTTP-Video applications.
94790	Fixed an issue where dataplane CPU usage became excessive after upgrading from PAN-OS 7.0 to PAN-OS 7.1.
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 an administrator deletes a vsys, the firewall automatically deletes NAT rules associated with that vsys.

Issue ID	Description
94573	Fixed an issue where a firewall dropped incoming PSH+ACK segments from the server.
94570	Fixed an issue where role-based Panorama administrators were unable to perform commits because the Commit dialog opened and immediately closed without allowing these administrators to modify, preview, or confirm their commit requests.
94533	Fixed an issue where Panorama pushed unused shared address objects to the firewall when the name of the object matched another pushed address object from the device group for that firewall even though the **Share Unused Address and Service Objects with Devices** option was unchecked.
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 could fail for jumbo packets.
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.
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.
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.
94097	Fixed an issue where the firewall did not log email sender, receiver, or subject in WildFire Submissions log.
93783	Fixed an issue 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.
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.
93729	Fixed an issue where SSH decryption caused a dataplane memory leak and restart.
93667	Fixed an issue 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**).
93458	Fixed an issue where WildFire platforms experienced non-responsive processes and sudden restarts under certain customer-specific traffic conditions.
93276	In PAN-OS 7.1.3 and later releases, the Application Command Center (ACC) includes the following usability enhancements: • You can **Jump to** Unified logs from an ACC widget; previously you could jump to all log types, except the Unified logs • You can easily promote an IP address or a user as a global filter from a table within an ACC widget. The context drop-down that appears next to the value allows you to promote the users or IP address as a global filter.

Issue ID	Description
93218	Fixed an issue where an administrator who is not a superuser was unable to view detailed configuration changes using **Logs** > **Configuration**. With this fix, administrators of all types are able to view detailed configuration changes.
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).
92684	Fixed an issue where a process (*l3svc*) stopped responding when processing a large number of user authentication requests.
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.
92467	Fixed an issue on Panorama where exporting the device state failed if a running-config.xml file already existed in the target location, which resulted in one or more `Server error` messages. With this fix, the new device state file exports as expected.
91726	Fixed an issue where using the hold and resume features during a call resulted in one-way audio when the call manager or SIP proxy was in a different zone than either the called or the calling party.
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.
91269	Fixed an issue where the firewall restarted the dataplane after a process stopped responding.
91202	Fixed a user interface issue on firewalls and Panorama where searches on Correlated Events logs using classless subnets (for example, /21 instead of /24) failed to give the correct results.
91171	Fixed the issue where, if the firewall processed a high volume of BFD sessions for routing peers that use BGP, OSPF or RIP, and the firewall also processed a high volume of packets belonging to existing sessions that were not offloaded, the BFD sessions to those peers flapped when the firewall received a content update.
91086	Fixed an issue where PA-7000 Series firewalls experienced BGP disconnections because the firewall failed to send keepalive messages to neighbors within specified timers.
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.
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.

Issue ID	Description
90596	Fixed an issue on PA-5000 Series firewalls where the FPGA did not initialize. With this fix, the FPGA is automatically reprogrammed after an initialization failure so that it can attempt to reinitialize (multiple times) before triggering a boot failure.
90560	Fixed an issue where the firewall did not authenticate a syslog server's certificate signed by a trusted root certificate authority (CA) included in the predefined trusted root certificate list, which caused connection issues with syslog forwarding over SSL. With this fix, the firewall can authenticate the syslog server's certificate and can establish SSL connections.
90508	A security-related fix was made to address CVE-2016-0777 and CVE-2016-0778 (PAN-SA-2016-0011).
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 before 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.
89984	A security-related fix was made to address a stack overflow condition (PAN-SA-2016-0024).
89551	Fixed an issue where User Activity Reports delivered via the Email Scheduler were empty if the username contained German language-specific characters.
89007	Fixed an issue where VM-Series firewalls deployed in AWS firewalls used UDP port 24946 for HA2 keep-alive packets instead of UDP port 29281.
88334	Fixed an issue where the firewall restarted unexpectedly when trying to delete a tunnel interface configuration.
88307	Fixed an issue where the dataplane restarted and dataplane processes stopped responding when passing SSH traffic using SSH decryption.
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.
88029	Fixed an issue where, after an upgrade, the firewall did not use the previously configured system-wide proxy configuration (**Device > Setup > Services**) for accessing the WildFire public cloud (PAN-OS 7.0 introduced a separate WildFire proxy configuration **Device > Setup > WildFire**). With this fix, the upgrade process automatically uses the previous proxy configuration when creating the WildFire public cloud configuration.
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.
83165 (PAN-49890)	Fixed an issue where exporting custom reports to CSV, XML, and PDF failed.
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.

PAN-OS 7.1.2 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.2 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Issue ID	Description
95120	Fixed an issue where authentication failed on the GlobalProtect gateway because the client tried to authenticate using cookies with domain\user specified in the agent configuration.
95021	Fixed an issue where the VLAN ID was added in the wrong location in the packet payload in Layer 2 deployments, which caused some applications to fail.
94990	Fixed an issue where the User-ID (*useridd*) process stopped responding when encountering a custom URL category that included a space (" ") character in the category name.
94939	Fixed an issue where strongSwan Linux VPN clients failed to connect to the GlobalProtect gateway because the firewall presented a server certificate that did not include a Common Name (CN) value.
94883	Fixed an issue on firewalls that were upgraded from a PAN-OS 7.0 release to a PAN-OS 7.1 release where GlobalProtect prevented third-party IPSec (X-Auth) clients from connecting to the GlobalProtect gateway. With this fix, you can now upgrade from a PAN-OS 7.0 release to a PAN-OS 7.1.2 or later release to prevent this issue. If your GlobalProtect firewall is already running a PAN-OS 7.1.0 or 7.1.1 release, you must downgrade to a PAN-OS 7.0 release before upgrading to a PAN-OS 7.1.2 or later release to prevent this issue from occurring after the upgrade.
94695	Fixed an issue where the firewall failed to connect to AutoFocus unless you manually re-entered the URL in the AutoFocus settings (**Device** > **Setup** > **Management**) even though the URL was correctly pre-configured. With this fix, the firewall connects to AutoFocus as expected using the prepopulated AutoFocus URL.
94571	Fixed an issue where commits failed if you configured two proxy IDs on a single tunnel using the same source, destination subnets, and protocol because the proxy IDs appeared to be duplicates of each other even though they were configured with different ports. With this fix, the firewall also uses the port value when determining whether proxy IDs are unique or duplicates.
94493	Fixed an issue where Panorama™ Device Group and Template administrators were unable to perform commits because the Commit dialog opened and immediately closed without allowing administrators to modify, preview, or confirm their commit requests.
94437	Fixed an issue where configurations pushed from Panorama running a 7.1 release to a firewall running PAN-OS 7.0 or earlier release incorrectly deleted the gateway configuration even when address objects were not included in the pushed configuration. With this fix, the gateway configuration is deleted only when the pushed configuration includes address objects.
94408	Fixed an issue where predefined URL categories were not populated in Security and Decryption policy rules as expected when using BrightCloud as the URL database.

Issue ID	Description
93961	Fixed an issue were 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).
93882	Fixed an issue where you were unable to deploy a VM-Series firewall using a VHD exported from an existing VM-Series firewall in Azure.
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.
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).
93526	Fixed an issue where the web interface and CLI reported that configurations were out of sync between HA peers even when the peers were in sync. With this fix, sync status is reported correctly.
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 7.1.2 or 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.
93395	Fixed an issue on firewalls and Panorama running a 7.1.0 or 7.1.1 release where the firewall *mgmtsrvr* or Panorama *reportd* process stopped responding and caused the process to restart after displaying the following message: `SYSTEM ALERT : critical : mgmtsrvr` (or `reportd`) `- virtual memory limit exceeded, restarting`. This issue was caused by a memory leak that occurred when viewing logs of single log types (such as Traffic or Threat).
93367	Fixed an issue where ACC logs did not resolve IP addresses to FQDN under destination IP activity.
93333	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.
93240	PAN-OS 7.1.2 and later releases are enhanced to prevent an issue where multiple SFP+ ports coming up at the same time resulted in a race condition that caused ports to enter a re-initialization phase that added several seconds delay before ports came up.
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.

Issue ID	Description
92979	Fixed an issue on Panorama where the **Administrator Use Only** option (**Template** > **Device** > **Radius Profile**) was not displayed in the web interface.
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.
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.
92642	Fixed an issue on Panorama (virtual and M-Series appliances) where a process (*configd*) stopped responding when triggering a commit very soon after a reboot and before a database required for the commit process was ready for use. Additionally, administrators received an error message (`Administrator does not have access to any device-group data`) when they attempted to view **Monitor** > **Logs** information or **ACC** information on the Panorama web interface before the database was ready. With this fix, this database loads faster so that commits and attempts to view **Monitor** > **Logs** and **ACC** information are successful even when attempted immediately following a reboot of Panorama.
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).
92391	Fixed an issue where firewall Traffic logs displayed unusually large byte counts for sessions passing through proxy servers.
92082	Fixed an issue where an administrator with read-only privilege was unable to export Correlated Events logs in CSV format.
92050	Fixed an issue on a PA-3000 Series firewall running a PAN-OS 7.0.1 or later release with zone protection configured to drop fragmented traffic where outgoing OSPF DB Description packets were fragmented and subsequently dropped, which caused the OSPF neighbor status to get stuck in Exchange state.
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 at the same time.
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.
91395	Fixed an issue where the simultaneous transfer of large files from two different SMB servers over a GlobalProtect connection from a Windows 8 client caused the connection to fail. With this fix, you can enable heuristics on Windows 8 clients or set the tunnel interface MTU size to 1,300 to avoid this issue.
91379	Fixed an issue where an out-of-sequence packet was passed through the firewall.
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 firewalls.

Issue ID	Description
91079	Fixed an issue on a VM-Series firewall where an ungraceful reboot caused Dynamic IP address information to get out of sync.
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.
90826	Fixed an issue where unused shared objects were calculated incorrectly during a commit from Panorama due to address and service name overlaps.
90044	Fixed an issue where log forwarding in Panorama failed when using syslog over TCP.
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.
89925	Fixed an issue where PAN-OS 7.1 images failed to bootstrap a firewall if the bootstrapping tarball package was created using a Mac OS (BSD-based tar format). With this fix, you can bootstrap firewalls with PAN-OS 7.1.2 or later release images using a BSD-based tarball created using a Mac OS.
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.
89261	Fixed an issue where you could not display interface QoS counters when the CLI output mode was set to `op-command-xml-output`.
88157	Fixed an issue with reduced throughput for traffic originating on the firewall and traversing a VPN tunnel.
86996	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.
86990	Fixed an issue on a firewall where a process (*sslvpn*) repeatedly restarted due to an internal thread synchronization issue.
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.
83722	Fixed an issue where destination-based service routes did not work for RADIUS authentication servers.
83569	Fixed an issue where multiple QoS changes while under a heavy load caused the dataplane to restart.
83339	Fixed an issue with the web interface where uncommitted IPSec proxy ID details were unexpectedly deleted prior to commit.
80177	Fixed an issue where the firewall did not present the URL block page as expected when proxied request from client used CONNECT method.
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.

Issue ID	Description
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.
40436	Fixed an issue where firewalls running PAN-OS 7.0 and earlier releases did not update FQDN entries unless you enabled the DNS proxy caching option (**Network** > **DNS Proxy** > *<DNS Proxy config>* > **Advanced**).

PAN-OS 7.1.1 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.1 release. Additionally, PAN-OS 7.1.1 introduces a new feature that provides Enhanced Security for Application and URL Category-Based Policy. For more new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Issue ID	Description
93710	Fixed an issue where the Pay-as-you-go (PAYG) hourly versions—Bundle 1 and Bundle 2 of the VM-Series firewall in Azure—were not available in the Azure Marketplace. These PAYG versions and solution templates are supported starting with PAN-OS 7.1.1.

PAN-OS 7.1.0 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.1.0 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 7.1 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.1.

Issue ID	Description
93072	A security-related change was made to address an issue in the policy configuration dialog (PAN-SA-2016-0014).
92382	Fixed an issue where the firewall could not install PAN-OS or GlobalProtect agent software images on leap day (February 29). With this fix, the firewall can install these images regardless of the date.
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.
91876	Fixed an issue where the passive firewall in a VM-Series ESXi configuration was processing and forwarding traffic.
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.
91728	A security-related fix was made to address a Denial of Service (DoS) condition related to the PAN-OS XML API (PAN-SA-2016-0008).
91653	Fixed an issue where SSL decryption did not work as expected for resumed sessions.
91533	Fixed an issue where a firewall failed a commit after receiving a File Blocking profile from Panorama that contained a space at the end of the profile name. This issue occurred when the managed firewall was running an older version of PAN-OS (when File Blocking and WildFire™ Analysis profiles were merged into one profile) and Panorama pushed the configuration to a device group.
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 can be edited.
91336	Fixed an issue where the packet processor stopped responding when proxy packets were switched to the fast path group on the dataplane.
91307	Fixed an issue where SSL decryption sessions failed for secure websites that used a certificate issued by the Entrust.net Certification Authority (2048).
91234	Fixed an issue on PA-7000 Series firewalls where a session was modified while in a state that should not allow modification, which caused processes associated with the packet processing daemon to stop responding.

Issue ID	Description
91075	Fixed an issue where the LSVPN tunnel interface started flapping after upgrading the firewall at one end of the tunnel (either the GlobalProtect gateway or satellite firewall) to a PAN-OS 7.0 or later release while the firewall at the other end of the tunnel was still running a PAN-OS 6.1 or earlier release. This issue occurred due to changes to encryption algorithm names when introducing Suite B ciphers in PAN-OS 7.0. With this fix, firewalls 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 stay up as expected.
91034	Fixed an issue on the WildFire platform where, if the snmp.log file is over 5MB, the snmpd process cleared the log file and restarted.
90982	Fixed an issue where upgrading from a PAN-OS 6.1 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 7.1.0 and later releases.
90933	Fixed an issue where the firewall generated superfluous logs (for traffic that did not match the configured filters) after you enabled dataplane debugging.
90857	Fixed an issue with a passive peer in an HA configuration where the web interface did not allow you to configure dynamic updates.
90794	Fixed an issue where a log file (/var/log/wtmp) inflated and consumed the available disk space. With this fix, PAN-OS uses a log rotation function to prevent log files from consuming more disk space than necessary.
90742	Fixed an issue where you could not add WF-500 appliance signatures as exceptions in an Antivirus profile when the signature names contained more than 32 characters.
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 Submission logs for non-NAT sessions contained incorrect or invalid NAT information.
90501	Fixed an issue where the firewall could not connect to a GlobalProtect portal or gateway after removing the LSVPN configuration.
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).
90411	Fixed an issue where a global counter (`flow_dos_pf_noreplyneedfrag`) related to the `suppress-icmp-needfrag` Zone Protection profile displayed the action as `drop` even when configured to `allow` ICMP Fragmentation. This fix introduces a new global counter (`Unsuprressed ICMP Need Fragmentation`).
90260	Fixed an issue where a device administrator was unable to configure certain settings under **Device** > **Setup** > **Operations**.
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
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.
90070	Fixed an issue where a memory leak associated with the authentication process (*authd*) caused intermittent access and authentication issues.
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 even though 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.
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.
89906	Fixed an issue where non-superuser administrators were unable to see Exempt Profiles and the Security policy rules in which the profiles are used when viewing a Threat log (**Monitor** > **Logs** > **Threat** > <*Threat Name*>).
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.
89752	A security-related fix was made to address a buffer overflow condition.
89750	A security-related fix was made to address a stack underflow condition.
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 WildFire deployment schedule.
89723	Fixed an issue where IPSec tunnels using IKEv2 failed to establish a VPN if multiple remote gateways were behind a port address translation (PAT) setup. With this fix, the firewall can allow multiple devices behind PAT to set up security associations to the same IP gateway.
89717	A security-related fix was made to ensure the appropriate response to special requests received through the API interface.
89706	A security-related fix was made to prevent some CLI commands from improperly executing code.
89595	Fixed an issue where attempting to **Hide Panorama background header** (**Panorama** > **Setup** > **Operations** > **Custom Logos**) resulted in an error (`Edit breaks config validity`).
89551	Fixed an issue where the User Activity Report did not show results for user names that contained German characters.
89503	Fixed an issue where user-group mappings were not properly populated into the dataplane after a firewall reboot.
89467	Fixed an issue with exporting a botnet report where exporting to CSV returned the `Missing report job ID` error.

Issue ID	Description
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.
89342	Fixed a rare condition where the root partition on a firewall or appliance ran out of space during device state generation.
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.
89284	Fixed a reporting issue on the ACC and SaaS Application Usage Report on managed firewalls. This issue occurred because the application information pushed from Panorama did not populate in a way or location that allowed the information to be used for reports generated on the firewalls.
89036	Fixed an issue where the `delete user-file ssh known-hosts` command was unavailable on an M-Series appliance in Log Collector mode.
88651	Fixed an issue where the User-ID (*useridd*) process stopped responding when the running-config was missing the port number associations for the Terminal Services (TS) Agent.
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.
88561	Fixed an issue where the tunnel went down and began to renegotiate, causing traffic destined for the tunnel during that time to be dropped. This issue occurred when the configuration was pushed from Panorama to a firewall configured with IKEv2 preferred mode and that was connected to a firewall configured to use IKEv1 in an IPSec connection.
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.
88408	Fixed an issue where the `show logging-status device` command used in the XML API caused the log daemon to stop responding when the device attribute was omitted.
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.
88313	Fixed an issue where read-only device administrators were unable to view logs on the **ACC** tab.
88279	Fixed an issue where the `debug dataplane packet-diag aggregate-logs` command showed an incorrect target filename.
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 now in place to control the log-cache size.

Issue ID	Description
88191	A security-related fix was made to address information leakage in system logs that impacted the web interface (PAN-SA-2016-0016).
88142	Fixed an issue with time calculation when displaying statistics for more than a single day (**Monitor > App Scope > Network Monitor**) that caused data to be unexpectedly shifted (calculation used 12:00 A.M. GMT instead of local time and data was shifted accordingly). With this fix, graphs display data across multiple days as expected for the local time on the firewall.
88141	Fixed an issue on Panorama where an administrator with an access-domain name longer than 31 characters received the following error when logging in: `Login could not be completed. Please contact the administrator.` With this fix, administrators with access-domain names of up to 63 characters can log in.
88101	Fixed an issue where WildFire reports (web interface and PDF) were unable to display digital signer information.
87911	Fixed an issue where scheduled dynamic updates to managed firewalls stopped functioning after migrating the Panorama VM to an M-500.
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.
87871	Fixed an intermittent issue in an HA active/active configuration where packets passed through a virtual wire were dropped due to a race condition that occurred when the session owner and session setup were not on the same HA peer.
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.
87851	Fixed an issue where high rates of fragmented packets caused the firewall to experience a spike in packet buffer, descriptor, and CPU usage.
87727	Fixed an issue where a virtual system custom role administrator could not add user to IP mappings using the XML API.
87594	Fixed an issue on M-Series appliances that caused the `show ntp` CLI command to time out.
87482	A security-related change was made to management plane account restrictions to prevent service disruption.
87414	Fixed a cosmetic issue where the `traffic` log type was displayed in the severity column of the Log Forwarding profile.
87207	Fixed an issue where the User-ID process (*useridd*) stopped responding, which caused the firewall to reboot.
87144	Fixed an issue where a change of an object name was not propagated in some parts of the configuration where the object was referenced.
87094	Fixed an issue where committing a policy on Panorama that contained interfaces that were manually defined generated an error: `[interface name] is not an allowed keyword`.

Issue ID	Description
87066	Fixed an issue on Panorama virtual appliances and on M-Series appliances in Panorama mode where two correlation engine sub-objects on the **Web UI** tab (Correlation Objects and Correlated Events) were incorrectly excluded when adding or modifying an Admin Role profile (**Template > Device > Admin Roles**).
86979	Fixed an issue where an incomplete IPSec tunnel configuration (one without an IKE gateway specified) caused the firewall server process to stop responding.
86977	Fixed an issue where LDAP sessions on Panorama were kept open and not actively refreshed. With this fix, a keep-alive mechanism is added that is triggered after 15 minutes of session inactivity and that allows a maximum of 5 failed probes before dropping a connection (probes occur in 60-second intervals).
86944	Fixed an issue on Panorama where a commit to a device group caused the Panorama job to fail, but the job was successful on the managed device.
86725	Fixed an issue where the SSL Certificate Errors Notify Page did not display values of some variables (such as `certname`, `issuer`, and `reason`) on web pages with expired certificates.
86717	Fixed an issue where QoS statistics for a specific interface were empty after a device reboot.
86686	Security-related fixes were made to address issues reported in the October 2015 NTP-4.2.8p4 Security Vulnerability Announcement.
86623	Fixed an issue where a firewall in an HA active/passive configuration dropped FTP PORT command packets after a failover.
86613	Fixed an issue where the General Settings dialog for **Device** > **Setup** > **Management** did not resize correctly when the Login Banner contained a large amount of text.
86488	Fixed an issue where predefined Application Usage Risk Trend graphs (**Monitor** > **Reports** > **PDF Summary Reports**) did not display lines between contiguous dots as expected.
86395	Fixed an issue where the administrator could not manually type the Ethernet interface name in a NAT policy in Panorama.
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.
85961	Fixed an issue that occurred when using the Panorama template stack where the configuration (gear) icon displayed in the wrong location (next to Panorama servers in the template stack).
85882	Fixed an issue where improperly formatted API calls to Panorama caused one of the system daemons to stop responding.
85602	Enhanced logging for events where long CLI system commands would timeout. For example, when generating a tech-support file.

Issue ID	Description
85426	Fixed a cosmetic issue where the log action for the interzone-default Security policy rule was incorrect in session detail (`session to be logged at end`) when the default log action was overridden by the user.
85344	Fixed an issue where scheduled dynamic update installation caused the HA link to flap.
85320	Fixed an issue where a process (*cryptod*) stopped responding when attempting to use SSH to access a firewall that rebooted into maintenance mode after the master key was allowed to expire. With this fix, administrators can use SSH to access the firewall without causing the cryptod process to fail even after a firewall reboots to maintenance mode after the master key expires.
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.
84911	Fixed an issue where an error was displayed when saving the NFS partition configuration on a Panorama virtual appliance.
84695	Fixed an issue where GlobalProtect was not appropriately indicated on the interface tab when it is configured on a loopback interface.
84414	Fixed an issue on the PA-7050 firewall where after deleting a HIP log forwarding profile a false warning would appear during a commit.
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.
84143	Enhancement made to allow administrators to include the application field and URL field in custom response pages.
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).
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.
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.
83239	Fixed an issue where inbound SSL decryption did not work as expected when you enabled SYN cookies.

Issue ID	Description
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.
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.
82524	Fixed an issue where a custom report with **Group By Source User** option did not include all data when the Source User field was empty.
82493	Fixed an issue so that the firewall performs NAT translations on IP addresses in an SCCP packet by doing a second NAT policy lookup instead of using a NAT policy for the current session.
82322	Added an enhancement to the PAN-OS routing engine for BGP routing protocol to remove a varying AS number preceded by a static AS number in the AS_PATH attribute.
82106	Fixed an issue where repetitive logging of inconsequential debug messages caused the snmpd.log file to reach its maximum file size and prevent further logging. With this fix, these inconsequential debug messages are no longer written to the log file.
80953	Fixed an issue where packets were not adhering to the virtual wire forwarding path, which caused MAC address flapping on neighboring devices. This occurred on a firewall in HA active/active virtual wire mode.
80750	Fixed an issue where you could not select a template stack or a descendant device group defined in a device group hierarchy on Panorama when specifying the device group and template for the VM-Series NSX edition firewall.
80336	Fixed an issue where Panorama custom report filenames that included a period (".") character resulted in empty reports. With this fix, reports are generated as expected for custom report filenames that include a period so long as the period is not the first character in the filename.
77273	Fixed an issue where importing a certificate with the same subject name as an existing certificate failed. With this fix, you can import a certificate that uses the same subject name as an existing certificate.
64717	Fixed an issue where an HA configuration did not correctly synchronize between firewalls when configured on Panorama and pushed to the firewalls.
42851	Fixed a performance issue with commit requests related to IKE configuration parsing. Also fixed cosmetic IKE validation messages displayed during the commit process, such as during a commit when the IKE gateway configuration was binded to an interface without an IP address. With this fix, the correct error message is displayed (`IKE gateway <gw-name> used local interface <interface> which has no IP address. Configuration is invalid.`)

Getting Help

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

▲ Related Documentation

▲ Requesting Support

Related Documentation

Refer to the following 7.1 documentation on the Technical Documentation portal or search the documentation for more information on our products:

- New Features Guide—Detailed information on configuring the features introduced in this release.
- PAN-OS Administrator's Guide—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls.
- Panorama Administrator's Guide—Provides the basic framework to quickly set up the Panorama™ virtual appliance or an M-Series appliance for centralized administration of the Palo Alto Networks firewalls.
- WildFire Administrator's Guide—Provides steps to set up a Palo Alto Networks firewall to forward samples for WildFire™ Analysis, to deploy the WF-500 appliance to host a WildFire private or hybrid cloud, and to monitor WildFire activity.
- VM-Series Deployment Guide—Provides details on deploying and licensing the VM-Series firewall on all supported hypervisors. It includes example of supported topologies on each hypervisor.
- GlobalProtect Administrator's Guide—Describes how to set up and manage GlobalProtect™.
- Online Help System—Detailed, context-sensitive help system integrated with the firewall web interface.
- 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 7.1
  - Panorama 7.1
  - WildFire 7.1

Requesting Support

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

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

Contact Information

Corporate Headquarters:

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054
https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 22, 2017