PAN-OS® 5.0.20 Release Notes

Revision Date: November 17, 2016

This release note provides important information about Palo Alto Networks PAN-OS software. To view a list of new features, refer to the New Features section. Refer to the Addressed Issues section for details on what has been fixed in each 5.0 release and view the Documentation Errata section for issues found in the documentation. Also review the Known Issues and the Upgrade and Downgrade Procedures thoroughly prior to installation.

Contents

New Features

This section provides details of the features introduced in the PAN-OS 5.0 release.

Note: Maintenance releases (where only the third digit in the release number changes, e.g. 4.1.0 to 4.1.1, or 5.0.0 to 5.0.1) do not include new features.

Application Identification Features

- **Application Dependency Enhancement—**For some protocols, you can now allow an application in security policy without explicitly allowing its underlying protocol. This support is available if the firewall can determine the application dependencies early enough in the session. For example, if you want to allow Java software updates, which use HTTP (web-browsing), you no longer have to explicitly allow web-browsing. This feature will reduce the overall number of rules needed to manage policies. This implicit support also applies to custom applications based on HTTP, SSL, MS-RPC, or RTSP. For a list of applications with implicit support, refer to the App-ID™ chapter in the *Palo Alto Networks Administrator's Guide*.

- **Traceroute Identification—**The App-ID software now identifies the traceroute application enabling the ability to easily control an application through policy. The following traceroute types are supported: TCP, UDP, and ICMP. Note that ping must be allowed if you want to allow traceroute over ICMP.

User Identification Features

- **User-ID Agent Enhancement—**This release incorporates all of the User-ID™ Agent functionality into PAN-OS. You can now configure the firewall to query the security event logs of your Windows servers and Novell NetWare servers directly for User-IP information. In addition, the firewall can now also act as a User-ID Agent for other firewalls and share the user-IP information that it collects. Note that the User-ID Agent installed on a Windows server can still be used, and is recommended in large deployments.

- **Dynamic Address Objects—**When creating an Address Object in PAN-OS, there is a new type called "Dynamic." Dynamic address objects do not have an IP address associated with them in the configuration file. Instead, when creating a dynamic address object, you specify an identifier that the XML API will use at run time to register IP addresses. This feature decouples security policy creation from the binding of actual IP addresses, which is useful in virtualized data centers where there is a high rate of change in virtual machine turn-up and associated IP address changes.

- User-ID XML APIs to register IP addresses are available both on PAN-OS and on the Windows-based User-ID agent. The maximum number of IP addresses that can be registered to a single dynamic address object is 256. The maximum number of IP addresses that can be registered to the dynamic address objects on a device is platform specific, and in a multi-VSYS deployment this limit is shared across all virtual systems. The maximum number of IP addresses for a platform is as follows:
    - PA-5000 Series—25,000
    - PA-3000 Series and PA-4000 Series—5,000
    - PA-200, PA-500, and PA-2000 Series—1,000

- **IPv6 Support for User-ID—**The following User-ID features now support IPv6: IP address to username mapping for the User-ID Agent, Captive Portal, User-ID XML API, and Terminal Server Agent. Additionally, IPv6 can now be used for communication between the User-ID Agent and the associated firewall.

Content Inspection Features

- **Palo Alto Networks URL Filtering Database (PAN-DB)—**PAN-DB is the Palo Alto Networks developed URL filtering engine and provides an alternative to the BrightCloud service. With PAN-DB, devices are optimized for performance with a larger cache capacity to store the most frequently visited URLs, and cloud lookups are used to query the master database. Daily database downloads for updates are no longer required as devices stay in-sync with the cloud.

- **Browse Time Report—**Some sections of the User Activity Report have a new column showing the estimated browse time for the listed categories or domains. To access this report, select **Monitor > PDF Reports > User Activity Report**. All existing user activity reports will automatically show the new browse time data moving forward.

- **IP Based Threat Exceptions—**Currently, threat exceptions are profile based, meaning that you exempt a specific signature for a specific profile. With this new feature, you no longer need to create a new policy rule and new vulnerability profile to create an exception for a specific IP address; you can now enter IP addresses directly in the threat exception to limit the exception to specific source/destination IP addresses. You will see the new IP Address Exceptions column when creating a new profile in **Objects > Security Profiles** for Anti Spyware and Vulnerability Protection profiles.

- **Dynamic Block List—**In the Objects tab, you can now select Dynamic Block Lists to create an address object based on an imported text file of IP addresses and ranges. These address objects can be used anywhere source and destination addresses are used in policy to block all traffic to and from any of the IP addresses on the imported list. You can also set an option to automatically import the list daily, weekly, or monthly. The source of the list can be an internal or external URL path, such as http://1.1.1.1/mylist.txt or you can enter a UNC server path. Each list can contain up to 5,000 IP addresses.

- **WildFire Subscription Service—**A WildFire™ subscription service is now available that enables the following capabilities:
    - **Hourly WildFire Signature Updates—**Enables you to receive WildFire malware signatures on an hourly basis. You can then control the action to take on the WildFire signatures.
    - **Integrated Logging—**WildFire results will also be logged directly into the Palo Alto Networks next-generation firewall logging system in **Monitor > Logs > WildFire**.
    - **WildFire API—**The subscription provides an API key to use the WildFire API to programmatically submit files directly to the WildFire cloud and query for analysis results. Users can send up to 100 files per day and query 1000 times per day with a single API key.

- **DNS-based Botnet Signatures—**DNS-based signatures detect specific DNS lookups for hostnames that have been associated with malware. You can enable/disable these signatures and create exception lists. The signatures will be delivered as part of the existing Antivirus signature database that is available through the threat prevention license. To control the action for these signatures, go to **Objects > Security Profiles > Anti Spyware Profile** and click the **DNS Signature** tab.

Decryption Features

- **Decryption Control—**A new Decryption Profile has been introduced with several options to provide better control over SSL and SSH sessions, including:
    - Block SSL sessions with expired server certificates.
    - Block SSL sessions with untrusted server certificates.
    - Restrict certificate extensions to limit the purposes for which the generated certificate will be used.
    - Block SSL and SSH sessions for unsupported modes (version, cipher suites).
    - Block SSL and SSH sessions on setup failures due to lack of system resources.

High Availability (Ha)

- **HA2 Keep-alive—**When configuring HA, you can now enable monitoring on the HA2 data link between HA peers. If a failure occurs, the specified action will occur (log or split data-path). The split data-path action is designed for active/active HA.

- **HA Path Monitoring Update—**New options have been added to specify the ping interval and number of failed pings required to initiate a path failure. Values are configured per path group. The current default values (200ms ping interval and 10 pings) will still apply unless custom settings are configured.

- **Passive Device Link State Control—**This enhancement improves failover times in active/passive deployments that make use of L2 or virtual wire interfaces by keeping the physical interface link state on the passive device in the link-up state. This feature already exists for L3 interfaces.

- **IPv6 Support—**HA control and data link support and IPv6 HA path monitoring is now available.

- **Dataplane Health Monitoring**—The PA-5000 Series and PA-3000 Series devices support an internal dataplane health monitor that will continually monitor all of the components of the dataplane. If a failure is detected, the device will attempt to recover itself after ceding the active role to the peer.

Networking Features

- **ARP Cache Increase—**The Address Resolution Protocol (ARP) cache on the PA-500 has been increased to 1000 entries and the ARP cache on the PA-2020 has been increased to 1500 entries. MAC tables have also been increased to match these values.

- **Link Aggregation—**The PA-500 and PA-2000 Series devices now support link aggregation. Note that link aggregation on virtual wire interfaces is not supported on the PA-2000 Series due to a hardware limitation. By assigning common ingress and common egress zones, two or more virtual wires may still be used on the PA-2000 Series in environments where adjacent devices are performing link aggregation.

- **Proxy ID Limit Increase—**The site-to-site VPN proxy ID capacity has been increased from 10 to 250 IDs per tunnel interface. On the PA-200 device, only 25 proxy IDs are supported. Note that each proxy ID counts toward the total VPN tunnel limit for a device. For example, the PA-500 device has a 250 proxy ID limit, so if you apply 125 proxy IDs each to two different tunnel interfaces, you will reach the overall limit for the device.

- **Symmetric Return (Return to Sender)—**This feature extends the functionality of Policy Based Forwarding (PBF) rules to circumvent the route lookup process and the subsequent PBF lookup for return traffic (server to client). The firewall will use the original incoming interface as the egress interface. If the source IP is in the same subnet as the incoming interface on the firewall, symmetric return will not take effect. This feature is useful when you have servers accessible through two ISP connections (on different ingress interfaces) and the return traffic must be routed through the ISP that originally routed the session.

- **Dynamic NAT Pool Enhancement—**Prior to PAN-OS 5.0, dynamic IP translation to two separate IP pools required you to specify two NAT rules and divide your internal addresses among them. The dynamic NAT pool enhancements feature enhances Dynamic IP translation (DIP) NAT rules by enabling you to specify multiple IP addresses, ranges, and subnets in the translated source field. A single dynamic IP NAT rule can now support up to 32K addresses.

- **Virtual Wire Subinterface—**You can now create virtual wire subinterfaces in order to classify traffic into different zones and virtual systems. You can classify traffic according to the VLAN tag, or VLAN tag plus IP address (IP address, IP range, or subnet).

- **Bad IP Option Protection—**In zone protection profiles, you can now specify options to drop packets with non-conformant IP options. Packets can be dropped if an IP option has the incorrect class, number, or length, and will be logged as *malformed option*. If the class and number are unknown, the log will indicate *unknown option*. In addition to dropping packets with malformed and unknown options, the firewall can be configured to drop packets with Security or Stream ID IP options. You can enable these options from the **IP Option Drop** section of the **Network** > **Network Profiles > Zone Protection > Packet Based Attack Protection** tab.

- **Remove TCP Timestamp—**A new option has been added to the Zone Protection profile to enable you to strip the TCP timestamp from the TCP header.

- **SLAAC—**Stateless Address Autoconfiguration (SLAAC) is now supported on IPv6-configured interfaces. SLAAC allows the firewall to send router advertisement (RA) messages on connected links in order to inform hosts of the IPv6 prefixes that they can use for address configuration. The firewall may act as the default gateway for hosts with this type of configuration. This option is available on all IPv6-enabled interfaces, except loopback and tunnel interfaces. A DHCPv6 server (external to PAN-OS) may be used in conjunction with SLAAC to provide DNS and other settings for clients.

- **IPv6 over IPSec—**This feature enables routing of IPv6 traffic over an IPSec tunnel established between IPv4 endpoints. You can use static routing or PBF to direct IPv6 traffic through IPv4 IPSec tunnels. This feature is useful when connecting IPv6 sites where an IPv6-capable WAN connection is not available.

- **NAT64—**NAT64 enables the firewall to translate source and destination IP headers between IPv6 and IPv4. It allows IPv6 clients to access IPv4 servers and also allows IPv4 clients to access IPv6 servers. This feature is now supported on Layer 3 interfaces and subinterfaces, tunnel interfaces, and VLAN interfaces.

GlobalProtect Features

- **Large Scale VPN—**The GlobalProtect solution has been enhanced to simplify the deployment of large scale VPN networks. The concept of a satellite device has been introduced, which allows a PAN-OS firewall to leverage configuration and credentials provided by a GlobalProtect Portal to dynamically establish VPN tunnels with GlobalProtect Gateways. The GlobalProtect Portal will automatically sign and rotate the satellite credentials used to authenticate to GlobalProtect Gateways.

- **X-Auth Support—**The following VPN clients are now supported for GlobalProtect VPN access:
    - Ubuntu Linux 10.04 LTS VPNC
    - CentOS 6 VPNC

- **GlobalProtect Agent Localization—**The GlobalProtect agent is now available in the following languages: Traditional Chinese, Simplified Chinese, French, Japanese, German, and Spanish. The language selection is based on the language set on the local computer.

- **Manual Gateway Selection—**In the GlobalProtect Portal client configuration, you can now set the option to allow the user to manually connect to a specific GlobalProtect Gateway. The Manual option can be selected when defining external gateways. When this option is set, the user can click the GlobalProtect agent icon and connect to any one of the defined manual gateways. When the connection to the manual gateway is initiated, the existing tunnel will be disconnected and a new tunnel will be established. This feature is useful if you have a group of users who need to temporarily connect to a specific gateway to access a secure segment of your network.

- **Pre-logon Connection—**The pre-logon option is part of the GlobalProtect agent configuration and is used to preserve pre-logon and post-logon services provided by a corporate infrastructure regardless of where the user machine is located. Use this option to create a logical network that maintains the security and management features normally achieved by a physical network. Tunnel selection and establishment occurs pre-logon based on machine certificates. Some of the services that can be maintained include: Active Directory group policy enforcement, drive mapping to server resources, and the ability to receive central software deployment downloads while working remotely. For example, the pre-logon feature is useful in the scenario where a remote user forgets his/her password. Because GlobalProtect connects and uses the cached credentials to establish a VPN connection before the login prompt even appears, a domain administrator could reset the user's password as if the administrator was logged in directly to a domain controller on the physical network.

Management Features

- **Translated Help—**The on-device Help content now contains the translated versions of the English content in the following languages: Chinese Simplified, Chinese Traditional, French, Japanese, and Spanish. The web interface language can be changed by clicking the Language link at the bottom right of the web interface window, or by navigating to **Device > Setup > Management > General** settings section and modifying the **Locale** setting. After changing the language setting, click the Help icon to access the help content for that language.

- **Visibility of Application Members in Policy—**You can now view detailed information on Applications, Application Functions, Application Groups, and Application Filters used in Policies from within the Policies page for Security, QoS, and PBF Policies by clicking on the Value option in the application context menu. This is useful, for instance, when editing a policy to discover application dependencies.

- **Minimum Password Complexity—**This feature allows you to define a set of password requirements that all local administrator accounts must adhere to, such as minimum length, minimum lower and upper case letters, requirement to include numbers or special characters, ability to block repeated characters and set password change periods. Select **Device > Setup > Management** to see the new options.

- **XML API Enhancement Import/Export—**The XML API for both PAN-OS and Panorama™ has been further expanded to support importing and exporting of files to and from the firewall and log retrieval. Also, in previous releases, only a superuser could use the API; now access to the API is provided for VSYS administrators, device administrators, and role-based administrators. Panorama administrators can also run device-targeted API queries.

- **XML API User/Group Mapping Enhancements**–The API can now communicate directly with the firewall to import user and group mapping data from systems other than a directory server. For example, you can have a database server that contains users and groups, but does not use an external directory server for authentication. In this case, you can create a scheduled script that uses the XML API to gather the user and group information and then imports this information into the firewall. After the information is imported, you can then create firewall policies based on these users/groups.

- **Scheduled Log Export via Secure Copy (SCP)—**When scheduling log exports, you now have the option to send the reports using an encryption protocol. In the **Device > Scheduled Log Export** and the **Panorama > Schedule Config Export** settings, you can now choose protocol SCP.

- **IPv6 Management Services—**IPv6 connectivity for administrative control has been added to PAN-OS and Panorama. When configuring management services from the web interface, the IP address fields will now accept IPv4 or IPv6 addresses. The following services are supported using IPv6:
    - Configuration.
    - RADIUS
    - Syslog
    - DNS
    - User-ID Agents
    - LDAP
    - SNMP
    - Panorama (device to Panorama connectivity)
    - SCP, FTP
    - SSH
    - Admin authentication sources
    - NTP
    - Panorama
    - Logging
    - Alerting
    - PBF next-hop monitoring of IPv6 addresses

    Note: TFTP is not supported because IPv6 support is not prevalent.

- **Certificate Management—**Enhancements have been made to improve workflow and management of certificates. The **Device > Certificates** section is changed to **Device > Certificate Management** and includes three new menus: **Certificates**, **Certificate Profiles**, and **OCSP Responder**. Some new features include the use of multiple OU fields when generating certificates, adding multiple alternate names, renewing certificates without regenerating keys, creating PKCS10 CSRs, revoking certificates, and the ability to enable/disable and export Default Trusted Certificate Authorities.

- **Graceful Shutdown and Restart—**The web interface has a new option in **Device > Setup > Operations** named **Shutdown Device**, which allows sessions to be logged prior to a shutdown. In addition, the **Restart Dataplane** option now allows the device to close and log existing sessions before restarting. You can also perform these operations from the CLI.

- **New SNMP MIB Objects—**SSL Decryption usage can now be monitored with two new objects: one for Total Active SSL Proxy Sessions, and another for SSL Proxy Session Utilization (as a percentage). Panorama connection status can now be monitored with new MIB objects. To utilize this feature, download the Enterprise SNMP MIB file for 5.0 from https://live.paloaltonetworks.com/docs/DOC-4120.

- **Web Interface Localization—**The PAN-OS and Panorama web interfaces are now available in the following languages: Traditional Chinese, Simplified Chinese, French, Japanese, and Spanish. The web interface language selection is based on the language set on the local computer that is managing the device.

- **Object Workflow Enhancements for Policies—**You can now view, edit, or remove objects defined in policies directly from the top-level policies page. For example, if you are configuring a security policy and need to modify the source address, you can click the down arrow to the right of the object and select Edit and the object properties will appear for editing.

- **Deep Matching in Policy Search—**When viewing the Policies tab and using the search filter bar to search policies, you can now search by an IP address (IPv4) contained within the values of objects or object groups. You can also search by IP range and subnet.

- **Packet Capture on the MGT Interface—**When running the operational command `tcpdump`, traffic through the MGT interface is now captured. To view the results, run `view-pcap mgmt-pcap mgmt.pcap`.

Panorama Features

- **Templates—**You can now use Panorama templates to manage device configuration options that are based on options in the Device and Network tabs, enabling you to deploy templates to multiple devices that have similar configurations. You can use a template to deploy a base configuration and, if needed, override specific settings on a device where customization is required.

- **Shared Policy Hierarchy—**This new feature adds the ability for Panorama admins to add an additional layer of pre and post rules that will be applied to all Device Groups managed by the Panorama instance. You can also set up admin access control options, so the rules are only editable by privileged admins and cannot be changed by Device Group admins.

  Another new feature for Shared Policy is the **Shared Objects Take Precedence** option, which is located in **Panorama > Setup > Management > General Settings**. When this option is unchecked, device groups override corresponding objects of the same name from a shared location. If the option is checked, device group objects cannot override corresponding objects of the same name from a shared location and any device group object with the same name as a shared object will be discarded. To access this feature, select the **Policies** tab and then select **Shared** from the **Device Group** drop-down.

- **Commit Workflow Improvements—**When selecting Commit on a Panorama device, you will now see a centralized commit window that is used to perform all commit functions. The new Commit drop-down items include:
  - Panorama—Commit changes made to the Panorama configuration.
  - Template—Commit changes made to templates. Each device that belongs to a template will be updated.
  - Device Group—Commit changes made to Device Groups. Each device or device/virtual system that belongs to the device group will be updated.

- **HA Device Awareness—**Firewalls in a high availability (HA) configuration will now be automatically identified by Panorama as a pair and will be visually grouped in Managed Devices, so when you add HA devices to a Device Group, you will just add the HA pair. Because policies pushed by Panorama are not synchronized by HA, this feature will make it easier to push polices by targeting the HA pair instead of accidentally pushing the changes to only a device in the pair. You will also see visual indicators, for example, if one device in a pair is not in the same device group as the other device, or if the devices do not have the same virtual system (VSYS) configuration. This feature is enabled by default; you can disable it by unchecking the **Group HA Peers** check box in **Panorama > Managed Devices**.

- **Share Unused Address and Service Objects with Devices—**This feature allows Panorama to share all shared objects and device group specific objects with managed devices. When unchecked, Panorama policies are checked for references to address, address group, service, and service group objects and any objects that are not referenced will not be shared. This option will ensure that only necessary objects are being sent to managed devices in order to reduce the total object count on the device. The option is checked by default to remain backward compatible with the current functionality of pushing all Panorama objects to managed devices.

Changes to Default Behavior

The following lists changes to the default behavior in PAN-OS 5.0 releases:

- In releases previous to PAN-OS 5.0.0, SNMP, HTTP, and Telnet management services were enabled by default. In PAN-OS 5.0.0 and later releases, SNMP, HTTP and Telnet management services are disabled by default and must be explicitly enabled (**Device > Setup > Management > Management Interface Settings**).

- The App-ID cache will no longer be used in security policies by default. For more information, see bug 47195 in the 5.0.0 Addressed Issues section.

- The workflow for adding threat exceptions from the **Monitor > Logs > Threat** details has changed. In prior releases, when you clicked the name of a threat in the threat log you would click the **Add to Threat Exception** button to define exceptions. In PAN-OS 5.0, you will now see a two-pane window in the threat log detail view. The left pane is where you can select an exempt profile that you configure in **Objects > Security Profiles > Vulnerability** (or **Anti Spyware**) and the right pane is used to define exempt IP addresses.

- The **IPv6 Firewalling** global setting in **Device > Setup > Sessions** is now enabled by default. In past releases, the setting was disabled by default.

- In earlier releases of Panorama, if you added an administrator and selected an Admin Role with the Role attribute set to Device Group and no device groups were selected, access to all device groups was granted. In 5.0, the new admin will not have access to any device groups if they are not explicitly selected. Additionally, the Admin Role has been enhanced to support templates and the previous Role of Device Group has been migrated to Device Group and Template.

- The `telnet` command is no longer available in the PAN-OS CLI.

- When configuring an LDAP Server Profile, entering the full domain as the server Domain name in an LDAP profile was allowed in PAN-OS 4.1.X releases (**Device > Server Profiles > LDAP**). Starting in PAN-OS 5.0.0, the server's NetBIOS domain name should be used when entering the LDAP server's **Domain** name, and not the full domain. For example, if your domain is paloaltonetworks.com, in PAN-OS 5.0.0 and later releases, enter `paloaltonetworks` (do not enter `paloaltonetworks.com`). A server's NetBIOS name is often the same as the system hostname, though this is not always the case. To confirm the server's NetBIOS name, you can use the command `nbtstat –n` in the command prompt or check the server's computer properties.

- When creating or modifying an LDAP server profile while running PAN-OS 5.0.0 and PAN-OS 4.1.X releases, the full domain name was required to populate the **Domain** field (**Device > Server Profiles > LDAP**). In PAN-OS 5.0.1 and later, enter the server's NetBIOS name in the **Domain** field for an LDAP server profile. Take the following steps to ensure that the **Domain** name field in an LDAP Server Profile is configured correctly for new and existing LDAP server profiles in PAN-OS 5.0.1 and later releases:
  - For existing LDAP server profiles configured prior to an upgrade to PAN-OS 5.0.1 or later, perform the following steps:
    1. Save the current configuration.
    2. Delete the existing LDAP server profile(s).
    3. **Commit** the change.
    4. Reload the saved configuration.
    5. Perform a second **Commit**.

    This workaround ensures that existing LDAP server profiles are configured correctly following an upgrade to PAN-OS 5.0.1 or a later PAN-OS 5.0.X release.
  - For a new LDAP server profile created when running PAN-OS 5.0.1 or a later release, use the NetBIOS name of the server as the LDAP server's domain name (not the full domain).

    For example, if your domain is paloaltonetworks.com, in PAN-OS 5.0.1 and later releases, enter only `paloaltonetworks`, not `paloaltonetworks.com`.

Upgrade and Downgrade Procedures

The following topics provide upgrade and downgrade procedures and details about how certain features are migrated.

Upgrade the PAN-OS Software Version

Important: To upgrade to a PAN-OS 5.0 release, the device must be running a PAN-OS 4.1 release. Attempts to upgrade to PAN-OS 5.0 from earlier releases are blocked.

Step 1: Update the Content Release Version

The device must be running content release version 370-4630 or later to upgrade to PAN-OS 5.0.7 or a later release and the device must be registered before you can perform an update to the content release version.

Note: If your device is not already registered, go to https://support.paloaltonetworks.com to register your device—you must have a Palo Alto Networks login to access this content. For assistance, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.

Use the following steps to perform a content update to the latest content release version, which consists of App-ID updates as well as threat updates, depending on your subscription licenses:

1. Select **Device > Dynamic Updates**.
2. **Check Now** to display the currently available content release versions.
3. **Download** the latest content release version.
   Note: If you have previously downloaded the same version, the Action column displays **Install** or **Revert** instead of **Download**.
4. After the download is complete, **Install** the new content release version.

Step 2: Upgrade the Software

Use the following steps to perform a software upgrade:

1. Ensure the device is connected to a reliable power source.
   Important: Losing power during an upgrade makes the device unusable.
2. Select **Device > Software**.
3. **Check Now** to display the currently available releases.
   Note: If you have previously downloaded the same version, the Action column displays **Install** instead of **Download**.
4. Locate the release version to which you want to upgrade and **Download** that version.
5. After the download is complete, click **Install** to perform the upgrade.

Downgrade the PAN-OS Software

Important: In a major release (where the first or second digit in the PAN-OS version changes, for example, from PAN-OS 4.0 to 4.1), the configuration can be migrated to accommodate new features. Do not downgrade unless you also plan to restore the configuration for that release. Maintenance releases (where the third digit in the PAN-OS version changes, for example, from PAN-OS 5.0.1 to PAN-OS 5.0.0) can be downgraded without restoring the configuration. Unmatched software and configuration can result in failed downgrades or even force the system into maintenance mode. If you experience a problem with a downgrade, enter maintenance mode and reset the device to its factory default configuration and restore the configuration from the original configuration file that you exported prior to the upgrade.

To downgrade the PAN-OS software:

1. Save a backup of the current configuration file:
    a. Select **Device > Setup > Operations**.
    b. Click **Export named configuration snapshot**, select **running-config.xml**, click **OK**, and rename the file. You can use this backup to restore the configuration if you have problems with the downgrade and need to perform a factory reset.
2. Downgrade the software version:
    a. Select **Device > Software**. The software page lists all the PAN-OS software versions available for download.
    b. Locate the desired release and **Download** that version.
    Note: If you have previously downloaded the same version, the active link displays as **Install** instead of **Download**.
    c. After the download is complete, click **Install** to perform the downgrade.
    Note: If downgrading to an earlier major release, when you click **Install**, you are prompted to select a configuration. For best results, Palo Alto Networks recommends using the configuration file backup you created before the upgrade or the auto-saved configuration file that was automatically created and saved when you upgraded to a major release.
3. Click **OK** to reboot the device and activate the new version.

For more information, refer to the Upgrading/Downgrading the PAN-OS Software section in the *Palo Alto Networks Administrator's Guide*.

Associated Software Versions

Software	Minimum Supported Version with PAN-OS 5.0.0
Panorama	5.0.0
User-ID Agent (AD)	3.1.0
User-ID Agent (LDAP)	3.1.0
Terminal Server Agent	3.0.0
NetConnect	Not supported in 5.0
GlobalProtect Agent	1.1

Addressed Issues

The following topics list issues address in PAN-OS 5.0 releases.

Addressed Issues 5.0.20

Note: Starting with PAN-OS 5.0.20, 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.

- PAN-64917—A security-related fix was made to address CVE-2014-9708 (PAN-SA-2016-0027).
- PAN-63073—Security-related fixes were made to prevent denial of service attacks against the web management interface (PAN-SA-2016-0035).
- PAN-61104—A security-related fix was made to address a local privilege escalation issue (PAN-SA-2016-0034).
- PAN-61046—A security-related fix was made to address a cross-site request forgery issue (PAN-SA-2016-0032).
- PAN-57659—A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0031).
- PAN-56221—A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0033).
- PAN-55259—A security-related fix was made to address multiple NTP vulnerabilities (PAN-SA-2016-0019).
- PAN-55237—A security-related fix was made to address an XPath injection vulnerability in the web interface (PAN-SA-2016-0037).
- PAN-55122—A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0021).
- PAN-52379—A security-related fix was made to address CVE-2015-5364 and 2015-5366 (PAN-SA-2016-0025).
- PAN-52038—A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0029).

- PAN-48954—Security-related fixes were made to address issues identified in the March 19, 2015 and June 11, 2015 OpenSSL security advisories (PAN-SA-2016-0033).

Addressed Issues 5.0.19

- 93612—A security-related fix was made to address a privilege escalation issue (PAN-SA-2016-0015).
- 93072—A security-related change was made to address an issue in the policy configuration dialog (PAN-SA-2016-0014).
- 92413—A security-related change was made to address a boundary check that caused a service disruption of the captive portal (PAN-SA-2016-0015).
- 92293—A security-related fix was made to address CVE-2016-1712 (PAN-SA-2016-0012).
- 88191—A security-related fix was made to address information leakage in systems log that impacted the web interface (PAN-SA-2016-0016).

Addressed Issues 5.0.18

- 89752—A security-related fix was made to address a buffer overflow condition.
- 89750—A security-related fix was made to address a stack underflow condition.
- 89717—A security-related fix was made to ensure the appropriate response to special requests received through the API interface.
- 89706—A security-related fix was made to prevent some CLI commands from improperly executing code.

Addressed Issues 5.0.17

- 86938—The client certificate used by PAN-OS and Panorama to authenticate to the PAN-DB cloud service, the WildFire cloud service, and the WF-500 appliance expired on January 21, 2016. The expiration results in an outage of these services. To avoid an outage, either upgrade to content release version 550 (or a later version) or upgrade PAN-OS and Panorama instances running a PAN-OS or Panorama 5.0 release to PAN-OS (or Panorama) 5.0.17 or a later release.
- 85065—Fixed a CLI input parsing issue that caused a process on the management plane to stop responding when processing unexpected input.

- 83519—A security-related fix was made to address CVE-2015-5600.

- 81367—A security-related fix was made to address CVE-2015-4024.

Addressed Issues 5.0.16

- 76238—A security-related fix was made to address CVE-2015-1873.

- 73790—Additional security-related enhancements were made to support frame-busting for the firewall web interface, in order to prevent framing of web interface elements.

- 73757—A security-related fix was made to enforce character encoding specified in HTTP headers due to CWE-116: Improper Encoding or Escaping of Output.

- 73638—A security-related fix was made to address issues related to HTML encoding.

- 73071—Fixed an issue where the firewall incorrectly sent duplicate SYN packets for ftp-data sessions.

- 72544—Addressed CVE-2014-8730. For additional information, refer to PAN-SA-2014-0224 on the Security Advisories site (https://securityadvisories.paloaltonetworks.com).

- 71486—A fix was made to address an issue with user input sanitization to prevent Cross-Site Scripting (XSS) attacks against the web interface.

- 71321—Removed support for SSL 3.0 from the GlobalProtect gateway, GlobalProtect portal, and Captive Portal due to CVE-2014-3566 (POODLE).

- 71320—Removed support for SSL 3.0 from the web interface due to CVE-2014-3566 (POODLE).

- 71273—A security-related fix was made in PAN-OS to address issues related to parsing XML data.

Addressed Issues 5.0.15

- 68708—Addressed the bash vulnerability CVE-2014-7169 that relates to how environment variables are processed when the shell starts up. This fix prevents a user with an account on the firewall, from using the vulnerability to gain escalated privileges.

- 66466—Addressed an issue for the PA-2000 Series platform, where a device failed to handle high volume of packets (larger than the MTU) on the management interface.

Symptoms of this issue included device unresponsiveness, a random restart, traffic failures or ATA errors on the console.

- 65607—If the last remaining user was removed from the Allow List for an LDAP authentication profile (meaning no users remained on the allow list), authd was not notified that the group was empty and retained the last user's information. That user could continue to be authenticated despite no longer be included in the allow list. This has been addressed so when the last user remaining on the allow list is removed, the user can no longer authenticate.

- 65146—Resolved an issue that occurred in high availability (HA) active/active mode, where HA3 packets could drop for a few seconds on the active-primary device while a content update was running on the active-secondary device.

- 58772—Performing a content upgrade appeared to result in an issue where traffic was failing to correctly match to a user group that was defined as the **Source User** in a security policy rule. This issue could not be reproduced, so an update has been made to provide further debug information to help troubleshoot the issue if it occurs again.

- 47761—Resolved an issue where the high availability (HA) flap counter was not resetting correctly; this lead to the maximum number of flaps being exceeded, and caused the device to go into suspended state. This issue is fixed so that the HA flap counter resets as expected if no flaps occur during the set period.

Addressed Issues 5.0.14-h3

Note:	If you have asymmetric routes in your network, before you upgrade to PAN-OS 5.0.14-h3, use the **set deviceconfig setting tcp asymmetric-path bypass** command to ensure session continuity. Additionally, if you have attached a zone protection profile, you must also execute the following command: **set network profiles zone-protection-profile <profile-name> asymmetric-path [bypass | global]**.

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

Addressed Issues 5.0.14

- 65643—When a firewall was configured with both 1GB and 10GB interfaces, and a 10GB interface went down, a backend process was not reporting the link down event instantly. An update was made to prevent the backend processes from delaying to report an interface's link status as down.

- 65156—Addressed CVE-2014-0224. For additional information, refer to “PAN-SA-2014-0003” on the Security Advisories site (https://securityadvisories.paloaltonetworks.com).

- 65146—Resolved an issue that occurred in high availability (HA) active/active mode, where HA3 packets could drop for a few seconds on the active-primary device while a content update was running on the active-secondary device.

- 64960—In a high availability (HA) active/active setup, when a device received Jumbo packets that had been fragmented, it transmitted the packets as fully assembled Jumbo packets. This issue has been resolved so that fragmented Jumbo packets are no longer transmitted as assembled Jumbo packets; both fragmented and assembled packets are transmitted correctly.

- 64553—When using the PAN-OS integrated User-ID agent, after the mapping has timed out, the firewall continued to send WMI probes to devices that were no longer responding. With this fix, the firewall does not perform WMI probing after the Time to live (TTL) for an IP address to username mapping expires.

- 64166—After approximately 388 days of uptime, the firewall lost the IP address to username mappings on the dataplane. This issue has been addressed so that the firewall does not lose IP address to username mappings when it reaches this uptime.

- 63971—Addressed an issue where the Network File System (NFS) process failed intermittently on PA-5000 Series devices configured in a high availability (HA) setup. This issue occurred because HA session updates were not being processed in the correct order and sessions were stalled. Though the issue was not specific to NFS traffic, it was more prevalent for NFS traffic and other application traffic with long session timeout periods.

- 62323—Made fixes to improve an issue where the firewall went into a non-functional state due to an out of memory condition caused by an internal process. Updates have been made to resolve some of the memory utilization issues.

- 62219—Unexpected XML data was present when loading an existing configuration version from the device resulting in a commit failure citing unexpected text. Update has been made to avoid this condition allowing successful commit when loading an existing Configuration Version.

- 61855—Resolved an issue where multiple configuration pushes from Panorama to managed devices could cause a managed device's management server to restart. When this occurred, a system log was generated showing show an increase in memory utilization for the management server. This issue is resolved so that commits from Panorama to managed devices succeed after for multiple configuration pushes and the management server remains stable.

- 47761—Resolved an issue where the high availability (HA) flap counter was not resetting correctly; this lead to the maximum number of flaps being exceeded, and caused the device to go into suspended state. This issue is fixed so that the HA flap counter resets as expected if no flaps occur during the set period.

Addressed Issues 5.0.13

- 63086—Resolved an issue that occurred in a high availability (HA) active/active setup, where the parent application sessions on a HA peer were not updated with traffic from the child application session and the parent applications sessions timed out. This caused the parent applications to close on both devices in the HA pair. This has been updated so that when the parent application session is refreshed on the primary device, it is now also refreshed on the secondary device.

- 62969—OCSP requests were using the OCSP location in the certificate instead of the location configured on the firewall. This has been adjusted so that the Palo Alto Networks next-generation firewall OCSP configuration will take precedence. If no OCSP location is configured on the firewall, the certificate OCSP location will be used.

- 62883—Addressed an issue where link state detection for a Fiber port on a PA-2000 Series device took 10 - 20 seconds.

- 62559—Resolved an issue where creating or modifying policy rules took a long time for large configurations (for example, a configuration with 3,000 rules and 20,000 objects). An update was made to increase the speed for creating and modifying policy rules for large configurations.

- 61879—IPSec VPN traffic could not be initiated following a restart of a system process. This issue has been resolved so that IPSec VPN traffic can be initiated even if the system process is restarted.

- 61827—Addressed an issue where a virtual wire with **Link State Pass Through** enabled had one interface that remained connected despite the other interface being physically disconnected.

- 61326—Addressed an issue that occurred in a high availability (HA) configuration, where link monitoring for a 10 GB port displayed the wrong status for the port when the port was down.

- 61284—Traffic using Policy-Based Forwarding (PBF) with symmetric return enforced experienced packet loss due to failed return MAC address lookups. This issue was caused by another change made in PAN-OS 5.0.11 which changed the PBF return MAC learning from the forwarding state to the session start; the PAN-OS 5.0.11 change that caused this issue has been reversed, which fixes the issue.

- 61101—Resolved an issue where the Address Resolution Protocol (ARP) table was not updated following Spanning Tree Protocol (STP) reconvergence in the network.

- 60681—Resolved an issue where a firewall tried to add entries to a log file that was not initialized. This resulted in the management server restarting unexpectedly. This issue has been addressed so that a check is performed to ensure that log files are initialized before entries are added to them.

- 59289—An issue has been addressed where dataplane restarts were seen due to PAN-DB becoming unresponsive. The dataplane instability was caused when new URLs could not be learned and repeated attempts increased the URL cache causing an excessive use of system resources.

Addressed Issues 5.0.12

- 62084—Addressed an issue where domain names greater than 63 characters were getting truncated in the resolv.conf file for Linux and Mac OS even when separated by commas.

- 61840—**Auth** and **priv** passwords defined for SNMPV3 setup on managed collector groups were displayed in clear text. With this fix, the passwords are masked and are not shown in clear text.

- 61828—TCP SYN cookies were activated sooner than the **Activate Rate** set in the DoS protection profile. Using DoS Protection with SYN cookies now activates correctly according to the configured SYN count.

- 61785—Fixed an issue where a virtual system administrator could delete logs for other virtual systems using the CLI.

- 61579—When session offload is disabled, the sequence and acknowledgement (SEQ/ACK) number check dropped ACK packets. This issue with the sequence and acknowledgement number check has been fixed in this release. The workaround for earlier releases is to use the command `set deviceconfig setting tcp asymmetric-path bypass`.

- 61383—A Panorama virtual appliance running PAN-OS 5.0.11 stopped processing logs. This issue was related to log migration errors and has been resolved so that logs forwarded to Panorama are processed correctly.

- 61168—SYN packets were dropped when a session with the same 5-tuple (same source IP address, destination IP address, source port number, destination port number, and protocol) was received by the firewall at the same time the existing

session was aged-out based on the TIME-WAIT period when source NAT (Dynamic-ip-and-port) was used.

- 60928—In certain situations on the Global Protect Gateway, the context for an IPSec tunnel to a Global Protect client shows presence of NAT-T, although there is no NAT between the client and the gateway. Traffic through that IPSec tunnel failed. The issue was caused when a tunnel context ID previously used for a tunnel with NAT-T was re-used for a tunnel without NAT-T. With this fix, tunnel contexts are properly cleared before re-use.

- 60781—A Dynamic Block List address object (0.0.0.0) was being added to security rules where that Dynamic Block List was referenced, even though that object did not exist in the Dynamic Block List source file. This was due to issues with EBL Refresh, and has been addressed so that when a Dynamic Block List is referenced in a security policy, the Dynamic Block List objects displayed in the policy are accurate.

- 60743—An untagged sub-interface caused stale hardware sessions on a PA-5000 Series device, and traffic failed when a new session was hitting the stale 5 tuple session. This issue has been fixed so that hardware session info is deleted when sessions are closed.

- 60700—1GB copper SFP interfaces belonging to an Aggregate Group would sometimes show the link status as down after a reboot of the firewall.

- 60673—LDAP groups containing non-ASCII characters in their names could not be processed by the firewall. Policies filtering on these groups were not working properly. With this fix, groups are received by the firewall, regardless of the types of characters used in their names.

- 60617—TCP connectivity issues occurred on a virtual machine when SYN Flood protection was enabled with SYN Cookies with the **Activate Rate** set to 0. This was related to an issue where active and passive FTP were not working under different NAT configurations and has been addressed so that both active and passive FTP work correctly under different NAT configurations and do not cause TCP connectivity issues. A workaround for this issue is to set the **Activate Rate** parameter for SYN Flood settings to a value greater than 0 (**Objects > DoS Protection > Flood Protection > SYN Flood**).

- 60505—SYN packets were dropped if a session with the same source and destination IP addresses and port and IP protocols comes to existing session at the timing of aged-out TIME-WAIT period.

- 60412—Unable to modify custom logo due to an unrecognized *mime-type* option (**Device > Setup > Operations > Custom Logos**). The fix adds the following option: *file -b --mime*.

- 60337—Fixed an issue where XML API showed empty hardware counters for dedicated HA1 interfaces after issuing the API query `<show><interface>dedicated-ha1</interface></show>`.

- 60274—Fixed an issue where the XML API showed an error after issuing the API query: `<show><high-availability><interface>ha1</interface></high-availability></show>.`

- 60201—In a high availability (HA) active/active setup, an IPSec key renegotiation timing issue caused the new IPSec session to be set to DISCARD until the next key renegotiation. This caused traffic loss until the next successful key renegotiation for the IPSec tunnel.

- 60189—When high availability (HA) active/passive peers lost communication on HA1 and HA2 links, a race condition caused the dataplane to restart.

- 60063—Certificate errors were seen when attempting to connect to certain sites with SSL Forward Proxy enabled; this was due to an issue with the Server Name Indication (SNI) extension within the client hello requests and the SNI extension was being dropped. This issue has been resolved so that the server is able read the SNI extension and respond to the client with the appropriate SSL certificates, and the client does not see any certificate errors.

- 60035—When an external zone was configured with a Zone Protection Profile applied to it, large IPv6 packets that traversed the zone were causing dataplane process failures.

- 59967—When the firewall was configured as a GlobalProtect satellite and was receiving access routes from another firewall configured as the GlobalProtect gateway, the routing resource counter for static routes was not incrementing or decrementing correctly. This behavior caused the maximum number of routes to be artificially reached and the firewall stopped accepting routing updates. The fix for this issue readjusts the counters for static routes and total routes when creating a redundant static route or deleting a non-existent one.

- 59890—When a PA-4050 firewall reached the limit for maximum supported concurrent decrypted sessions, the dataplane restarted. A fix has been added to ensure that the device will stop decrypting sessions once the limit is reached and a restart will not occur.

- 59772—Traffic logs from managed log collectors were not visible on the Panorama web interface.

- 59180—Session set up between a client and server was not completed in a high availability (HA) active/active environment when configured with multiple virtual systems and multiple virtual routers. The client from one virtual system could not reach the server located on a second virtual system because the session in the second virtual system was not set up correctly.

- 59018—A network outage occurred when the number of active sessions reached 100,000 sessions. This occurred on a PA-3000 Series firewall and Detector Threats have been increased on PA-3000 Series firewalls in order to address this issue.

- 58421—PA-500 firewalls infrequently experienced unexpected restarts with an NMI watchdog error on the console.

- 57736—Active FTP through NAT (Dynamic IP/Port) did not work on a virtual machine. This issue has been addressed so that both active and passive FTP work under different NAT configurations.

- 57601—Fixed an issue where Data Filtering logs were showing incorrect file names when the data pattern was matched against the files.

- 50798—Device fans running at lower speeds were sometimes causing a thermal alarm. This occurred when the dataplane restarted while the device was in a temperature alarm state. In this case, the fan's speed control value was set to the default value, causing the fan to run at the incorrect speed. This issue has been addressed so that the fan speed is recalculated based on the device's current temperature following a dataplane restart.

- 48758—In some cases, large amounts of compressed HTTP traffic could cause the zip buffer to fill so that it was unable to process additional compressed HTTP traffic. Offload of compressed HTTP traffic now works correctly so that even large amounts of compressed HTTP traffic are processed by the zip buffer.

Addressed Issues 5.0.11

- 59949—Issuing the command `clear user-cache ip <ip>` did not clear the IP-to-user cache on the dataplane for non-vsys1 virtual system when in multi-vsys mode.

- 59873— A TCP session could not be established when SYN Cookies was enabled when both Aggregate and Classified DoS Protection Profiles were configured.

- 59618—Attempting to download packet captures for traffic displayed an error that the file was not found. This issue was seen when the IPv6 address had the full 128 bits in the address. This has been fixed so that the packet capture file now correctly displays the contents of the PCAP file on the web interface.

- 59574—Fixed an issue where an Antivirus profile on Internet Explorer and Firefox browsers was not showing the default action in parenthesis (alert/drop/) for the decoders.

- 59556—Fixed a memory-related race condition in high availability (HA) configurations that was contributing to Control Plane restarts.

- 59336—Performing a local commit on an active pair and then a high availability (HA) sync caused the management server memory to increase on the passive pair.

- 59328— Unable to sort Managed Collectors by Collector Name on the Panorama web interface, in either ascending or descending order (**Panorama > Managed Collectors**).

- 59256—Performing an SCP import of the logdb file failed with the error: `failed to verify for logdb import`.

- 58971—The CLI output for the command `show routing protocol bgp loc-rib-detail` displayed the community field incorrectly when certain prefix combinations appeared in the IP addresses of the BGP neighbors.

- 58656—A bad disk in an M-100 appliance was causing the system to reboot. With this fix, the error: `Startup script failure` is not shown in the masterd_detail.log.

- 58586—Was unable to log into the web interface. A root partition on an M-100 was at 100% usage due to old reports being incorrectly stored in the /tmp directory.

- 58421—Following an upgrade from 4.1.11 to 5.0.5, some firewalls infrequently experienced unexpected restarts.

- 58255—Import of logdb file on the firewall failed. The issue happened in certain cases due to old purged logs. In these cases, the firewall importing the logdb is looking for the purged logs in the logdb and the import fails.

- 58095—When trying to access a firewall using Panorama as a role-based administrator, the dynamic updates screen did not populate.

- 58029—On a PA-5000 Series firewall deployed in high availability (HA) active/active scenario, it was possible for the first SYN packet of the ftp-data session to be dropped.

- 58003—A virtual machine stopped passing traffic when a dead-lock condition was reached. This caused the comm process to miss too many heartbeats and exit out with a core. This fix makes sure that the deadlock is detected, and by allowing a pan_task core dump, prevents any outages due to this deadlock.

- 57997—The User-ID agent status is displayed as `connected` on the active-secondary device in a high availability (HA) environment. The expected behavior is to show as `disconnected` and this issue has been fixed so that the expected behavior occurs.

- 57920—A PA-5000 Series firewall was dropping EtherIP traffic when excessive fragmentation was encountered.

- 57411—Applying a Policy-Based Forwarding (PBF) rule with Symmetric Return and a Source NAT rule to traffic entering the firewall was causing return traffic to be dropped.

- 57380—Fixed an issue where Panorama stopped processing logs from firewalls after getting a register message from the firewall.

- 53422—SSL Forward proxy was blocked with Certificate Error (Status: expired) when cert was not expired. This was due to a race condition.

Addressed Issues 5.0.10

- 58627—In situations where a Panorama log collector failover occurred, some logs were lost during the failover to the secondary collector and then the failover back to the primary collector.

- 58616—When the appinfo2ip cache was full and the command `show running appinfo2ip` was issued, a short network outage occurred.

- 58539—When using GlobalProtect pre-logon mode, an administrator was unable to log a user out from the web interface or the CLI and the session did not time out correctly. This was caused by an issue relating to different domain names being configured for the certificate profile and the authentication profile. This issue was fixed so that domain names are properly converted and users log out and time out as expected.

- 58387—IPSec VPN traffic was sometimes dropped when custom proxy-IDs were configured on a virtual machine.

- 58386—A dynamic block list configured to access a HTTPS URL was causing the test command on the web interface to fail.

- 58324—Captive Portal NTLM authentication sometimes failed if there was a communication issue between the firewall and User-ID Agent.

- 58257—Admin Role features could not be disabled while configuring a custom admin role.

- 58061—An LDAP authentication profile was being used to authenticate GP clients. Authentication was successful but the firewall was not sending password expiration notifications to the client. This occurred when space characters were used when configuring the LDAP authentication profile. The issue has been resolved so that authentication continues to be successful and password notifications are sent to the client regardless of whether space characters are used in the LDAP authentication profile.

- 58006—When the firewall received fragmented packets and sent them to an IPSec tunnel, the firewall would further fragment the original packets in order to fit the ESP header. However, the firewall would not set the more fragments (MF) bit in all packets where it's needed. This resulted in packets being reassembled on the receiver side.

- 57972—Fixed an issue where the address object in a NAT rule was removed after an upgrade.

- 57816—Groups were not displayed in the Allow List dropdown selection of an Authentication Profile. This was due to changes made for an issue addressed in PAN-OS 5.0.7 (49237). This issue has been fixed so that groups are displayed in the Allow List dropdown selection of an Authentication Profile for single-vsys devices.

- 57763—When WildFire Action was configured as "default(Block)" in Antivirus profile, block action didn't take effect as the default action was not configured internally. The workaround is to configure WildFire Action as "Block" instead of "default(Block)".

- 57762—When using NTLM authentication for Captive Portal the redirect page sometimes failed when accessing websites using HTTPS. The browser was displaying a page with the error stating that NTLM Authentication had failed due to the user failing to enter the proper credentials too many times.

- 57612—SSH sessions to servers running OpenSSH version 6.2 or newer through SSH Decryption were failing in some instances when the computed Diffie-Hellman key is 4096 bits.

- 57549—Fixed an issue in the web interface where the application filter was not working correctly on the **Objects** > **Applications** page.

- 57544—Exporting logs using SCP consumed more management plane memory and took longer in Panorama 5.0.X releases, compared to Panorama 4.1.X releases. The high memory usage sometimes caused a management server restart. Improvements were made to reduce the total time to export logs.

- 57538—Management server memory usage increased on a firewall when addressed objects or policies were pushed from Panorama. A fix was made to stabilize the management server memory on the firewall.

- 57402—Virtual wire interfaces on the passive device with passive link state set to auto were flapping following a HA-SYNC job completion. Issue has been fixed so that IFMon will be aware of high availability (HA) passive-link-state setting.

- 57263—Fixed an issue where the search queries in group mapping profiles resulted in the error message: `missing server`.

- 57196—On PA-3050 and 5000 series, in certain situations when NAT is applied to FTP traffic, the FTP Close message could be transmitted with incorrect checksum.

- 57059—An IP Spoofing check for Zone Protection did not work when SYN Cookie was enabled.

- 56995—The error message `external is invalid signed-by` was displayed when attempting to generate a CSR External Authority certificate with the firewall in FIPS mode. As a result, this prevented the CSR External Authority certificate from being generated (**Device** > **Certificate Management** > **Certificates**).

- 56810—The dataplane would sometimes unexpectedly restart after a configuration commit if the interface configuration is added or changed.

- 56481—Fixed an issue where the incorrect data is displayed in the web interface traffic logs for the HTTP-proxy application.

- 56429—In an active/active pair and with jumbo frames enabled, a fragmented packet sent over the HA3 link was reassembled for inspection, was not defragmented, and was sent back out as jumbo frames.

- 56153—Packet loss occurred when an IP packet larger than 1480 bytes passed through a high availability (HA) active/active vwire setup.

- 54649—An unexpected restart occurred on a managed device after pushing a device group configuration from Panorama to the managed device. The restart was caused by a race condition that occurred when committing.

- 53443—On the **ACC** tab in the web interface, the URL Filtering chart continued to load indefinitely when attempting to display large amounts of URL information or items (for example, 500 items).

Addressed Issues 5.0.9

- 57645—Certain scheduled custom reports contained no data when they were generated.

- 57343—Fixed an issue that caused improper handling of imported certificates that contained HTML.

- 57277—An administrator using the Panorama web interface was unable to preview changes when performing a commit on a managed device.

- 57147—Using Panorama to push a source NAT rule with a Dynamic-IP to a managed device running PAN-OS 4.1 caused a commit to fail on the managed device and displayed an error.

- 57143—If the original parent session could not be found, the firewall was dropping ICMP error messages even when a policy was configured to allow ICMP error messages to be sent through the firewall.

- 57111—When the web interface was set to display in a language other than English, the order in which policy rules were listed could not be changed by using the Move Up or Move Down options.

- 57015—On a PA-2050, the dataplane board agent virtual memory usage was observed to be steadily increasing.

- 57056—The next hop information for VPN tunnels was not synchronized between the high availability (HA) peers. This caused the passive device's next hop table to fill to the limit and the firewall would not have been able to process VPN traffic if a failover had occurred.

- 56766—In vwire mode, URL block pages generated by the firewall could be transmitted using unexpected source MAC addresses.

- 56644—When using the REST API to retrieve WildFire verdict logs from Panorama, the first request for the logs worked as expected and returned response status and response code and the job ID. The second request to get the output of the job ID took several minutes to complete and did not return any error or response code or data.

- 56479—Performing a commit sometimes failed if management CPU utilization was high.

- 56476—The web interface displayed an error when attempting to set the location of a container page to an existing virtual system. The existing virtual system could not be

selected despite meeting all the conditions for a valid object name described in the error.

- 56203—Certificates with the secure hash algorithm sha384 generated an error when performing a commit.

- 56003—SQL sessions were not connecting through a firewall when a data-filtering profile was enabled.

- 55951—Traffic logs were dropped due to the firewall switching log collectors when the primary log collector went down. The traffic logs were dropped until a connection to a backup log collector was established.

- 55949—Under certain circumstances, GlobalProtect Portal authentication failed when using two factor authentication.

- 55702—An unexpected system restart was caused by a kernel change from PAN-OS 4.1 to PAN-OS 5.0.

- 55580—In an agentless User-ID configuration, a periodic WMI Probe did not start automatically after clearing the user cache.

- 55367—When SSH Forward proxy was enabled and a user created an SSH session, the session disconnected after being idle for 20 minutes. This did not occur when SSH Forward proxy was disabled.

- 55287—When a RADIUS user's administrator permission scope was set to Device group and template, the permission was not being enforced correctly and shared objects could be modified using the web interface.

- 55284—In the web interface, attempting to add the same proxy server domain name to more than one DNS Proxy resulted in an error. This has been fixed so that DNS Proxies can be configured with their DNS Proxy Rules including the same Domain Name.

- 55157—A firewall in an active/passive high availability (HA) cluster restarted unexpectedly. A preventative check was introduced so that if the session pointer is NULL, it will no longer be dereferenced and will not cause an unexpected restart.

- 55018—When the Palo Alto Networks URL filter (PAN-DB) would run a dynamic query for an unknown URL, proxy server settings were not used.

- 54987—The firewall was retransmitting SYN packets when it received packets with a destination IP address from the Palo Alto Networks next-generation firewall source NAT

IP pool, resulting in a loop. This issue has been fixed so that the firewall does not learn the ARP entry when the source IP in the ARP packet belongs to its source NAT IP pool; the firewall will not forward packets with a destination IP address that belongs to the Palo Alto Networks next-generation firewall source NAT IP pool.

- 54767—In the REST API, the command `show running resource-monitor minute/day/hour/second/week last x` was not displaying resource monitoring statistics for DP1 or DP2.

- 54407—User group names with extended formats were not being parsed correctly and could not be added to a security policy as source users. The user group names were being truncated and the entire names were not displayed.

- 54317—A VLAN interface configured as a DHCP client in IKE Gateway configuration resulted in the error message: `Configuration is invalid` when attempting to commit.

- 54000—The ARP entries associated with a Layer 2 interface that is a part of a Layer 3 VLAN interface were not cleared from the ARP table when the Layer 2 interface went down.

- 53843—After changing the DNS server settings on a firewall, the firewall was not using the new DNS server settings for OCSP DNS lookups.

- 53451—DNS proxy responses served by the firewall for static entries were using a very high TTL value. The TTL for static entries has been changed to 7 days.

- 52922— When configuring SNMPv3 on a high availability (HA) cluster, configuring the Engine ID using the **EngineID** field syncs the primary device's Engine ID to the secondary device (**Device** > **Server Profiles** > **SNMP trap**). To maintain unique Engine IDs on the primary and secondary device, leave the **EngineID** field empty. This issue was originally addressed in PAN-OS 5.0.7 and updates were made at that time that were specific to that release.

- 52549—The dataplane was generating URL logs for denied traffic even though no URL filtering profile was configured for the applicable policies. A fix was made to generate URL logs only when URL filtering profiles are applied.

- 51971—Issuing the PASV command did not modify the client passive IP Address to the NAT IP address of the server. This issue has been fixed so that Passive FTP works on a firewall with NAT configured.

- 51322—When captive portal was prompted for an HTTPS session, but there was no matching decryption policy to decrypt the session and no matching security policy to

allow the traffic, the session was denied. However, PAN-OS did not properly close the proxy server connection with RST, resulting in an exhaustion of resources on the proxy server. This issue has been fixed so that an RST is sent to the proxy server when a captive portal redirect cannot be sent.

- 51203—Zone protection profiles were not activating when applied to external zones in a Shared Gateway environment.

- 49182—When using the Panorama web interface to reboot a device, the web interface became unresponsive until the device was fully rebooted. This was due to failures not being detected while requests were being sent to the device. The Panorama web interface now continues to be responsive during the period before the device is fully rebooted and after the device is rebooted.

- 40876—When configuration logs were exported to CSV, some columns expected to be in the report were not displayed, including the columns Before Change and After Change.

Addressed Issues 5.0.8

- 56832—Radius Authentication failed after upgrading to PAN-OS 5.0.7. An issue occurred with internal structures when validating the access domain object.

- 56279—Code changes have been made to accommodate a change in the date that daylight savings takes effect for Israel Standard Time (IST) to the new date of October 27th.

- 56062—A packet buffer leak was occurring after upgrading to PAN-OS 5.0.7. This was due to an issue where software packet buffers were not freed and caused the software packet buffer pools to be unavailable for packet processing.

- 56030—Automatic IPv6 packet captures were not being saved. The problem was due to filenames containing ";", which caused the device to not recognize the packet captures.

- 55971—An internal path monitoring script exited unexpectedly and caused a system restart. This has been resolved so that the ‘exit’ condition does not cause a system restart.

- 55898—The Log Details window for specific log entries was not correctly displaying Japanese file names and related logs.

- 55778—URL Filtering was not working for URLs that contained certain Japanese characters.

- 55775—In the web interface, an application filter's characteristics in a security policy (**Policies** > **Security** > **Application Filter**) were not shown to be consistent with the same application filter's configured characteristics displayed in the **Objects** > **Application Filters** > **Application Filter** window.

- 55765—In a high availability (HA) active/active configuration with session setup set to IP Modulo, some software memory pools were becoming saturated and memory could not be freed.

- 55698— REST API configuration operations set against a template value resulted in an error: `set failed, may need to override template object first`. Support for override operations has been added to the REST API.

- 55614—An Antivirus profile was not working when it was applied to a custom application.

- 55582—In the web interface, the **Commit** icon was enabled when there were no pending configuration changes. This has been fixed so that the **Commit** icon is enabled only when pending configuration changes are available to commit.

- 55579—Addressed an issue where IPSec tunnels configured with an ID greater than 4096 were causing tunnels to fail due to corruption of the encap/decap context table. Each SPI pair is tied to a unique Context ID, and the corruption of the context table was causing the duplication of the SPI pair.

- 55574—After deleting a custom response page, the **Commit** icon was not activated.

- 55441—Importing a PKCS #12 certificate using the Panorama web interface failed when the Passphrase contained special characters.

- 55389—The previous maximum limit of rows for CSV Export was 65535. The maximum limit of rows that you can set for CSV Export has been increased to 1048576 (**Device** > **Setup** > **Management** > **Logging and Reporting Settings** > **Log Export and Reporting**).

- 55354— Removing the Shortest Path Tree (SPT) parameter in an existing multicast configuration failed upon commit. This was due to a race condition and caused the router daemon to stop responding.

- 55273— When using agentless User-ID to redistribute IP address to username mappings to connected firewalls, deleting an IP address to username mapping using the XML API was not causing the same IP address to username mapping to be deleted on the firewalls connected to the Collector. This has been resolved so that using the

XML API to delete an IP address to username mapping, successfully deletes the IP address to username mapping on connected firewalls.

- 55195—In some corner cases, URL categorization requests sent to the management plane for http-proxy sessions failed to be processed correctly, resulting in the device-server process restarting.

- 54964—Fixed a dataplane restart issue that occurred when processing RTSP traffic.

- 54906—When using a Policy-Based Forwarding (PBF) rule with symmetric return, if the return-mac table was nearly full, a race condition was causing a new entry to not be added to the table, which caused traffic not to flow.

- 54879—When importing a custom welcome page for GlobalProtect, the firewall allowed upload of .png files even though they are not a supported file type for the welcome page.

- 54848—When a FQDN object was added to the destination address in a security policy, changing the FQDN in the address object was causing the original FQDN to be blocked instead of the new one.

- 54791—Even when a user's IP address is in the Exclude list of the Zone User Identification ACL, sometimes the excluded user was still being displayed in the traffic logs.

- 54776—In the Panorama web interface **Monitor** > **Logs** > **Traffic** tab, if the user entered a search query for several days back in time, the query could take 20 or more minutes to return if there was a large amount of log data stored.

- 54539—In the web interface **ACC** tab Threat Prevention section, clicking one of the icons in the Severity column of an entry caused the message `No Matching Record` to display. This has been fixed so that the icons cannot be selected.

- 54439—High CPU usage on Panorama was causing the CLI and web interface to become unresponsive after login, requiring a restart. This was due to an issue where warning and error messages were not being correctly deleted for previously committed configurations. Operations to delete warning and error messages for previously committed configurations have been optimized so that they require less time and do not use high CPU.

- 54399—With an LDAP profile configured to use SSL, the system logs showed that the User-ID Agent was connecting using the management interface even though the service route for a User-ID Agent was set to use a dataplane interface.

- 54347—Extremely large amounts of traffic (exabytes, or billions of gigabytes) were showing up in the **ACC** tab and logs for users. An issue where the date of record showed as starting in 2031 caused the incorrect counter of traffic, due to the date being set in the future. Date verification is now supported to prevent this from occurring.

- 54279— VPNC client software connected to the GlobalProtect gateway using Xauth only allowed the Security Association (SA) lifetime to be negotiated to 8 hours. The reuse login lifetime default remains 8 hours. However, additional functionality has been added so that you can set the reuse login lifetime to a minimum of 24 hours or more. Use the new command `set global-protect xauth-reuse-login-lifetime on|off` to turn the reuse login lifetime option on or off. Issuing the command `set global-protect xauth-reuse-login-lifetime on` causes the Login Lifetime configured in the web interface (**Network** > **GlobalProtect** > **Gateways** > **GlobalProtect Gateway** > **Client Configuration**) to be used as the reuse login lifetime instead of the 8 hour default.

- 53962—Network performance issues were occurring with GlobalProtect agents connected to a GlobalProtect gateway. The issues occurred because the Maximum Transmission Unit (MTU) on the ingress interface of the gateway was changed to 1404, but the Maximum Segment Size (MSS) sent to GlobalProtect agents was not updated properly, causing fragmentation issues. An update was made to ensure that the MSS is adjusted properly when the ingress interface MTU is changed.

- 53938—Resolved an issue with some SIP video phones that would result in one-way video on occasion.

- 53746—Path monitoring on the VM-Series firewall was not working as firewall was monitoring destination IP address "d.c.b.a" incorrectly when the actual IP address was "a.b.c.d".

- 53231—WildFire dynamic update images were not removed after being downloaded to a Panorama server that was used to push the images to managed firewalls. The expected behavior is that the last five images should be kept and then deleted as new images are downloaded.

- 52134—Spanish-language characters were not being properly parsed by the firewall when received from a firewall configured with Agentless User-ID, causing the user to not be matched to the correct rule. This issue has been resolved by extending support for ASCII characters for WMIC.

- 51853—In the Panorama CLI, authenticating a custom role-based account using RADIUS caused the following error message to display: `Server error: show -> system -> setting -> multi-vsys is unexpected test@Panorama>.`

- 50813—DNS proxy fails to proxy traffic with bursts of DNS requests, displaying the error: `(errno: 105) No buffer space available`. This was resolved by increasing the buffer.

- 49931—An unexpected reboot occurred while collecting tech support information from a PAN-OS device.

- 47417—The user interface took an excessive amount of time (greater than 3 minutes) to display virtual routers in a PAN-OS configuration with a large number of virtual routers (greater than 125). This occurred on the web interface **Network** > **Virtual Routers** tab.

- 47032—GlobalProtect authentication failed when using a client certificate profile with a name that contained special characters (in this case, Spanish-language accented characters). This was due to the UTF-8 format being the only string input format supported in certificate creation. String input format support has been extended to include bmpString in order to resolve this issue.

- 46399—Using the Panorama web interface to clone a default or strict profile security profile was resulting in the following error: `1- Failed to clone default. Could not find schema node for xpath /config/predefined/profiles/vulnerability/entry[@name='default']`. The error occurred when attempting to clone the default or strict security profiles for Antivirus, Anti-Spyware, Vulnerability Protection, and URL Filtering.

Addressed Issues 5.0.7

- 54619—Wildfire logs were not available for export from the CLI using SCP or FTP in the CLI.

- 54585—Two administrators with the same privileges were able to take simultaneous config locks when the first config lock was taken using the web interface and the second config lock was taken using the CLI.

- 54490—When using the web interface to add a group mapping configuration (**Device > User Identification > Group Map Settings**), the search field to add Available Groups to the Include List was not displaying Available Groups or returning search results.

- 54413—On the M-100 appliance in Distributed Log Collection architecture, a slight difference was noticed between the disk capacity available on the RAID disks and the available capacity identified in memory. This issue caused the M-100 appliance to exceed the maximum log storage quota allotted, and in some cases resulted in the disk becoming full. This issue is now fixed.

- 54368—Enforcement of the application override policy for a custom application was occasionally failing, resulting in the traffic logs showing the custom application as “unknown-tcp” instead of identifying the application as the custom application defined in the application override policy.

- 54336—The maximum number of rows that can be set to appear in comma separated values (CSV) reports is 1,048,576, with the default number of rows being 65,535. In the web interface, even when the maximum number of rows to appear in CSV reports is set as 1,048,576, the command `scp export log traffic max-log-count` was limiting the number of rows exported to the default (65,535). Using the command `scp export log traffic max-log-count 1048576` allows the maximum number of rows (1,048,576) to be exported.

- 54164—In the GlobalProtect VPN client, if the Palo Alto Networks LDAP authentication Password Expiry Warning and LDAP server maximum password age are set to more than 127 days, the standard warning popup displaying the password expiration age failed to appear. This was due to the maximum password age being limited to 127 days; it can now be set to up to 255 days.

- 54146—After creating and then adding a FQDN address object to a security rule, the output for the `command request system fqdn show` displays the FQDN object as unresolved. This issue only occurred if the FQDN resolved to 10 or more IPv4 and 10 or more IPv6 addresses.

- 54141—Committing a critical high availability (HA) group configuration was resulting in an email alert following commit: “SYSTEM ALERT: critical: HA Group 1: Running configuration not synchronized after retries”. A timeout on the HA peer while committing the HA synchronization caused the email alert to be generated.

- 54072—In the Panorama web interface, changing the default number of configuration backups to save before discarding the oldest ones was committing successfully but the updated number of configuration backups to save was not displayed in the field **Number of Versions for Config Backups** under the **Panorama > Setup > Management > Logging and Reporting Settings > Log Export and Reporting** subtab after the commit.

- 54032—The web interface became unresponsive when a user operating in a custom administrator role (not the default super user role) saved a policy configuration.

- 54002—After pushing template objects from Panorama to a managed device, and then importing the template settings to the managed device and disabling the Panorama Device and Network Template, the imported objects remained read-only and could not be edited.

- 53991—After upgrading PAN-OS software in an active/passive high availability (HA) configuration, the active firewall was unable to obtain the version information from the passive peer. This was occurring even though the passive firewall was able to determine the OS version of the active firewall.

- 53808—After installing a content package and performing a FQDN refresh, the configured user to group mapping on the dataplane appeared to no longer be configured and the output of the command `show user ip-user-mapping ip` was displaying the error message “groups info is outdated”.

- 53701—In the web interface, deleting all users and user groups from the Allow List of an Authentication Profile caused “all” to become the default Allow List for that Authentication Profile. After committing the change, the Allow List column in the web interface was showing “all” as the default, but this rendering was not the same as the running configuration. The running configuration did not have the same default attribute as the web interface and this caused some user access issues. The default “all” has been removed and there is no default Allow List.

- 53638—Security policies configured using Host Information Profiles (HIP) to identify users were failing to be enforced in an active-passive high availability (HA) configuration.

- 53616—Using the web interface to set the time zone of the device to the Europe/Minsk time zone was displaying the error message “Unable to connect to device”. This occurred only when attempting to set the time zone to the Europe/Minsk time zone.

- 53445—Taking a config lock with the Panorama option set as the location of the lock was failing to block configuration changes. The Panorama option was removed from the dropdown selection of possible lock locations as it offered no additional functionality.

- 53353—The web interface was incorrectly displaying a shadow rule warning during a successful commit. This was occurring when an existing DoS policy was cloned, the cloned DoS policy’s service attribute was modified, and a commit was performed.

- 53271—Pushing a template from Panorama, where a Virtual System was assigned to an external zone, to a managed device was resulting in an invalid reference error and the commit was not completed on the managed device. This was due to the managed device failing to recognize the Virtual System’s display name, instead of the Virtual System ID.

- 53258—Authenticating access to a file share folder hosted outside of the Active Directory domain was causing the firewall to change the User-IP Mapping to the username and password used to authenticate to the file share folder hosted outside of the Active Directory domain, instead of the Active Directory username and password.

- 53254—The output for the command `show system disk space` was not correctly displaying file system disk space usage. The command has been fixed so that the output displays all information correctly.

- 53251—When the web interface language was set to any language other than English, the error message “Panel for undefined not registered” was displayed in the popup **Combined Rules Preview** after clicking **Preview Rules in Policies > Security > Pre Rules**.

- 53197—Symmetric return under Policy Based Forwarding (PBF) did not work with a DHCP configured interface. It performed correctly with a static IP address configured on the same interface.

- 53188—The User-ID feature was unable to connect to an Active Directory server. This occurred when the user was trying to connect to the Active Directory server.

- 53187— The firewall dropped IKE traffic where another IKE session was in the discard state on the firewall. Since the tuple for the new session matched the session in the discard state, the packet for the new session was dropped and the session in discard state was refreshed. This caused the discarded session to linger for a longer period of time that is longer than normal. The session will linger as long as there is traffic being received that matches the session (5 tuple) because every time the session is received, PAN-OS refreshes the session timeout.

- 53177—Values in the multicast FIB table for a firewall were different as displayed in the web interface and in output from the CLI command: `show routing multicast fib`.

- 53141—When the firewall received a BGP update message from a BGP peer with AS value “0” inside the AS_PATH aggregator attribute, the BGP connection was dropped by the firewall. The behavior under these circumstances was changed to drop the BGP update message instead of closing the BGP connection with the peer.

- 53124—The captive portal session cookie timeout value was set to an unrealistically high value after the firewall device was up for one week.

- 53123—Several unscheduled custom reports created by the customer were configured on Panorama running on an M-100. Even though the reports are configured to unscheduled, they were run on a daily basis.

- 53108—In rare instances, a PA-200 firewall went into maintenance mode after a power outage instead of performing a normal reboot as expected.

- 53027—Although a factory reset was performed on a firewall to set the master key to the default value, the master key remained the same as before factory reset. This occurred only when the master key was changed manually.

- 53020—When using URL filtering with ssl-decrypt url-proxy enabled, denied websites displayed an action of "allow" in the URL logs instead of "deny" even though the user would see the URL block page.

- 52967—The firewall inappropriately transmitted WMI probes from the User-ID function by default.

- 52954— The firewall was unable to categorize some of the customer URLs. Because these URLs were not categorized, the firewall could not block them where required. This occurred because the transmission buffer maximum size from management plane (MP) to data plane (DP) was too small in some rare situations where a URL exceeded the maximum size. Consequently, categorization for the URL domain did not propagate into the dataplane. This has been corrected by increasing the transmission buffer maximum size from management plane to dataplane.

- 52922—When configuring SNMPv3 on a high availability (HA) pair, configuring the Engine ID on the primary device automatically synced the same Engine ID to the secondary device. This was changed in order to maintain unique Engine IDs on the devices and so that the Engine ID sync from the primary device to the secondary device does not occur; the Engine ID must be configured independently on both primary and secondary devices.

- 52920—In an active/active high availability configuration, the HA3 link was assigned to an aggregate Ethernet interface. In this configuration, IPv6 TCP packets were not sent back to the firewall that had received the first packet from the primary device. These packets were sent if a single (non-aggregate) Ethernet interface was used for the HA3 link.

- 52905—The Continue page was not displayed as expected although "url-proxy" was enabled on the firewall and "Forward Trust CA" was configured.

- 52890—The Load Filter icon adjacent to the search bar on the **Monitor > Logs** page of the firewall web interface did not appear when the page was opened. It would appear when the page was scrolled. With this release, it will appear when the page is opened and not require scrolling to view it.

- 52885—Registration of firewall from the **Setup > Support** page failed and issued the following error message: “Invalid username or password”. This occurred when using a password that contained special characters.

- 52870—The firewall experienced high CPU utilization when the User-ID service was enabled with a large number of IP address-to-user mapping and multiple firewall clients connected.

- 52790—The column header in a PDF summary report that should be titled “Website” was displayed as “Country” instead.

- 52787—Session filtering by source zone or destination zone could not be performed using the firewall web interface in a multi Virtual System environment where the zones being configured were not in VSYS1.

- 52781—Configuration export was configured in Panorama to export a file from a firewall to a destination host using the SCP protocol. This export failed when the destination host offered only a DSA key signature. The same operation succeeded when the host offered an RSA key signature. This issue has been resolved so that the configuration export is successful when the host offers a DSA key signature or an RSA key signature.

- 52751—When a very large number of user activity reports were run from Panorama, the following message was generated: “mgmtsrvr – virtual memory limit exceeded, restarting”.

- 52724—The 802.1q tag was missing on the transmit interface for multicast traffic. This happened because the VLAN tag was not set on the Layer 2 interface for multicast forwarding packets.

- 52664—When an NSSA area External Range was configured to suppress the external routes from the firewall web interface in the Virtual Route - OSPF - Area configuration, the external routes were not correctly suppressed.

- 52633—A vulnerability profile was created in Panorama on an M-100 and it was then pushed to a firewall. The profile that was pushed from the M-100 did not appear in the exceptions tab of the Vulnerability Protection Profile on the firewall.

- 52624—Addressed a link state issue in a high availability (HA) setup when a virtual wire was configured and the link state on the passive device was enabled for pass through. In this scenario, when the link on an interface failed, the link state for both interfaces was not brought down. With this fix, when one interface in a virtual wire pair goes down, the link state for both interfaces in the virtual wire displays as down and the failover is successfully triggered.

- 52606—When defining a security policy on Panorama, the icon that displayed for user groups was inaccurate. With this fix, the icons on Panorama accurately represent user groups from individual users.

- 52574—The M-100 intermittently stopped responding after an admin used the search functionality within a device group tab.

- 52570—On the PA-5000 Series, addressed an error in processing traffic when multiple virtual systems were configured and traffic traversed between the virtual systems.

- 52546—Addressed an issue in the FPGA that caused a buffer overflow for jumbo frames on the PA-5000 Series. With this fix, buffer utilization and flow control thresholds were updated to prevent buffer overflow.

- 52536—Addressed a restart on the User-ID process that occurred when the XML API was used to add or delete users.

- 52530—Addressed an authentication issue that occurred when a Cyrillic username was configured in the local database. With this fix, UTF-8 encoding for Cyrillic characters has been added.

- 52490—In policy, if the “/” was used for URL matching (for example google. */*), all characters after the “/” were overlooked. With this fix, the URL match criteria evaluate all the characters defined in the expression.

- 52447—Addressed an issue on the VM-Series firewall where software packet buffers cloned for App-ID processing were not freed and caused the software packet buffer pools to be unavailable for packet processing.

- 52422—Certificates could not be successfully generated if the certificate name or the common name defined in the certificate was more than 255 characters. This issue is now addressed and both these fields now support up to 1024 characters.

- 52383—The User-ID agent lost domain name information for some users when the NetBIOS domain name and the AD domain names were different. With this fix, the domain map is retrieved so that domain names are accurate for all users/ groups.

- 52286—On the PA-2000 Series, fixed dataplane stability issues that were caused by excessive memory utilization on the dataplane.

- 52272—Botnet reports did not display the full URL. With this fix, URLs will not be trimmed in botnet reports.

- 52268—Threat logs did not accurately reference the policy rule that triggered the log entry.

- 52213—On the PA-500 in an active/passive high availability (HA) configuration, the next hop information for VPN tunnels was not synchronized between the HA peers. This caused traffic to stop being processed on failover.

- 52205—On the **Panorama > Managed Devices** tab, the status of a device for which a template commit has never been pushed from Panorama displayed as Out of Sync (in the template column). This issue has been addressed, and Panorama does not report In Sync or Out of Sync status for a device that has not been configured using Panorama templates.

- 52182—Fixed a restart issue that occurred when the firewall was configured for OSPF routes.

- 52126—On-demand and scheduled custom reports, on an M-100 appliance in Panorama mode, were generated as empty reports. With this fix, the report is populated with the requested data.

- 52085—Creating packet capture filters for subinterfaces with names longer than sixteen characters was failing due to a 16-character limit on subinterface names. The 16-character limit on subinterface names was removed in the CLI in 5.0.6 and removed from the web interface in 5.0.7.

- 52040—The firewall lost the IP address-to-user name mapping when the group mapping information was refreshed. With this fix, the firewall successfully retrieves group mapping information.

- 52028—In a high availability configuration, the active-secondary peer in the active/active case or the passive peer in the active/passive case unnecessarily refreshed the parent session. The issue prevented the device from creating new sessions.

- 52025—Addressed an issue on the PA-3000 Series and PA-5000 Series where the TCP checksum was calculated incorrectly when NAT was performed.

- 52010—Addressed an authentication issue that caused a timeout and blocked Internet access for users when captive portal was enabled.

- 51911—Addressed an issue with the order in which URL lookups were performed. With this fix, a URL lookup uses the following order: block list, allow list, custom categories, and pre-defined categories. This means that if a URL belongs to a block list and to a custom category, the block list should apply since it is evaluated first in the lookup order.

- 51898—Intermittent Captive Portal authentication issues occurred after restarting the User-ID agent on the domain server. Recovery mechanism put in place to resolve this issue.

- 51854—Device Groups administrators who were authenticated by a RADIUS server using RADIUS Vendor Specific Attributes, were unable to commit changes to Panorama although they had commit access. This issue is now resolved.

- 51782—The router daemon on a passive device in a high availability (HA) active/passive configuration intermittently stopped responding when a port on the active device continually flapped due to a switch problem. This caused multiple route changes and HA sync updates, which eventually caused the route daemon issue. Update made to better handle this type of issue.

- 51667— The system log retention details for an M-100 appliance that was deployed as a dedicated Log Collector were not displayed accurately from the web interface or CLI on Panorama. This issue is now addressed.

- 51658—If an SSL decryption policy was enabled and an OCSP responder was configured for checking the revocation settings of the decryption certificate, SSL traffic was denied because all certificates were treated as untrusted.

- 51494—On failover in a high availability (HA) configuration, traffic that was blocked by policy was not correctly synchronized between the peers. This caused sessions that were denied and discarded on the active node to be allowed on the passive node.

- 51352—When trying to filter logs in Panorama based on the generated time field, no results appeared after applying the filter, even though a valid time was being used. Update made to allow this operation for all Panorama log types.

- 51322—When a network with a large number of Mac computers had a Palo Alto Networks firewall with Captive Portal configured between the Mac clients and a secure proxy server, issues occurred when the Mac computers continually sent http/https requests to an Apple site for online help purposes. When 100+ Mac computers sent these requests to the Apple servers simultaneously, the firewall would open connections to the Apple server for Captive Portal redirection purposes, which maxed out the proxy server and caused issues with other users connecting to the Internet. Because Captive Portal requires a successful log-in to continue the client session, there is no need to allow these requests from the firewall to the destination server, so an update has been made to send an RST to the server and client when a Captive Portal log-in fails.

- 51103—The User-ID process stopped responding on the active device after a high availability (HA) active/passive failover. This occurred when group mapping was configured and was caused by a null pointer issue for the group mapping on the passive

device. Not able to reproduce in-house, but an update has been implemented to resolve the null pointer issue.

- 51080—Certificate errors occurred after mistakenly importing a PA-2020 4.1 configuration to a PA-3050 device running PAN-OS 5.0. Issued occurred because the import removed two required directories that contain certificate information. This is a rare situation and to avoid this issue, do not import configurations from different hardware with different versions of PAN-OS.

- 51058—Performance issues were occurring on a PA-5000 Series device with zone protection enabled while under a DoS UDP flood attack with packets per second exceeding 100k. Issue due to a problem with packet buffers queues not being evenly distributed among the dataplanes.

- 50992—A custom application signature written for ICMPv6 type 1/2/3 with the application-default set for the service was not working properly. Unknown IPv4 traffic was also matching the rule with the custom app and the logs showed the IPv4 traffic as incomplete and insufficient-data. Issue due to a problem recognizing the ICMPv6 protocol, which has been fixed.

- 50597—When selecting multiple rules and then clicking the Clone button, the new cloned rules were listed in reverse order. For example, if you have three rules named test1, test2, and test3 and you use the ctrl key to select all three rules and then click the Clone button, the new cloned rules should appear as rule1, rule2, rule3. Before this fix, they appeared as rule3, rule2, rule1, which was in reverse order.

- 50095—The Panorama API browser was incorrectly displaying a link for User-ID. The link has been removed since User-ID is not applicable to Panorama.

- 50074—A Panorama administrator account configured with admin role permissions while in version 4.1 could no longer perform a commit-all after Panorama was upgraded to 5.0. Issue was due to an update to 5.0 that requires the role-based admin to have permissions to device groups and templates before a commit-all can be performed. With this fix, the role-based admin is granted read-only access to device groups and templates, so a commit-all can be performed.

- 49920—Resolved a memory issue that was occurring in Panorama when five or more admins were simultaneously logged in and performing various tasks, such as viewing logs and App Scope as well as connecting to managed devices. This caused an issue where memory was not freed up and continued to increase.

- 49376—When a re-key occurred on a VPN tunnel between the Palo Alto Networks firewall and a Juniper SRX, the tunnel stopped functioning for a short period of time, causing packet drop. Update made to prevent this issue.

- 49371—Addressed a restart that occurred when the XML API on the firewall was frequently used to retrieve information using the GET action. These GET actions placed the memory utilization under heavy load and caused a management server restart.

- 49237—When configuring a shared authentication profile, user to group mapping information gathered by LDAP/Radius were available when adding members to the auth profile, which did not allow authentication for the members. This should not have been an option, only virtual system specific authentication profiles should be able to use this type of group. Update made to not display these groups when configuring a shared authentication profile.

- 48630—HIP Match logs that were being pushed from a managed firewall to Panorama were not displayed on the Panorama web interface (in **Monitor > Logs > HIP Match** section) despite the managed device displaying that the HIP Match logs were being sent.

- 42024—Update made to PAN-OS to support Server Name Indication in SSL Forward Proxy decryption.

Addressed Issues 5.0.6

- 52913—Additional management plane statistics were added in PAN-OS 5.0.3 to help identify and diagnose memory issues; in PAN-OS 5.0.6, these monitoring statistics have been enhanced to support all released versions.

- 52698—The dataplanes on PA-5000 Series and PA-4000 Series firewalls stopped responding soon after the BrightCloud URL filtering database was updated and the URL category refresh was performed. This occurred when the URL dataplane cache was extremely large, which caused a memory issue. Update made to perform the category refresh in smaller increments when a large number of URLs are present in the cache.

- 52613—Fixed a restart that occurred when processing the H.245 protocol.

- 52566—When adding a source user to a security policy, the drop-down list that contains the list of users was not sorted properly.

- 52381—When Agentless User-ID was configured to exclude a network used for Captive Portal authentication, captive portal logins from the excluded network were not added to the user to IP address mapping table, and could therefore not be applied to the user access policy. The fix for this issue is to ignore Captive Portal-based logins when evaluating the Include and Exclude lists.

- 52368—Softphones were not receiving DHCP option 150 from a Cisco DHCP server when traffic passed through the firewall. This issue is resolved and all DHCP options are now supported.

- 52322—When a user was prompted with a Captive Portal prompt with NTLM enabled and then successfully authenticated, on some occasions the user was prompted to authenticate again. This was observed with the Internet Explorer browser.

- 52309—When modifying a security policy using the web interface, the web interface would sometimes become unresponsive.

- 52255—Using the Run Now function to run a user activity report on a device worked correctly; however, clicking Run Now to generate a user activity report for Panorama or scheduling user activity reports on either Panorama or a device was resulting in User Activity Reports that were limited to 5000 rows. This occurred regardless of the maximum number of rows that were configured in Logging and Reporting settings to support user activity reports.

- 52249—A zone protection profile with the SYN cookies option enabled failed to allow TCP connections to complete correctly after upgrading from PAN-OS 5.0.4 to 5.0.5. This occurred on a PA-5000 Series device and was due to an issue forwarding data between data-planes.

- 52085—Creating packet capture filters for subinterfaces with names longer than sixteen characters was failing due to a 16-character limit on subinterface names. The 16-character limit on subinterface names has been removed in the CLI and will be removed from the web interface in an upcoming release.

- 52006—In a TCP session, the TCP wait timer could be set to a maximum of 60 seconds. There is now the capability to set the TCP wait timer above 60 seconds, with a new maximum of 600 seconds. Note that setting the TCP wait timer above 60 seconds will delay the timeout of TCP sessions by that amount, causing session utilization to increase.

- 51908—After configuring an application exception for an antivirus profile and applying that profile to a security policy, the application exception was not functioning properly.

- 51779—When a Panorama template, with the Force Template Values option enabled, was used to push dynamic update schedules to managed devices, the update schedule was not applied on the managed devices if the devices were manually configured with a schedule. With this fix, the dynamic update schedule pushed from Panorama is applied to the managed devices and the settings on the device are in sync with the template.

- 51713—Applying a BGP AS path filter caused the router daemon on the firewall to stop responding, causing a high CPU condition. This was caused by a looping condition.

- 51644—A commit failure occurred on Panorama when pushing NAT Policy with dynamic IP address(es) to managed devices running PAN-OS 4.1.

- 51412—When using the XML API to view QoS interface throughput statistics on a PA-5000 Series firewall, the XML command would fail because it was not supported by the service that handles statistics output on that platform. Support has been added for QoS throughput statistics so that the XML command is now successful.

- 51348—In rare instances, attempts to commit changes to the virtual router configuration would cause the firewall to stop responding. This resulted from a lock condition that occurred with a specific configuration.

- 51281—PAN-OS was not handling certain SSL error messages correctly. This has been fixed so that SSL error messages are no longer causing policy bypass.

- 51263—An M-100 appliance was receiving traffic logs from a managed device but the logs were not present in the database. Received logs were not being properly inserted into the database on the M-100 appliance. Received logs will now be added to the database when multiple messages arrive on the same target process.

- 51225—When an interface was configured with hard-coded options, such as setting the duplex to full instead of auto, the interface did not come back up after a reboot. The same interface worked fine after setting it to auto negotiate. This occurred on a PA-2020 firewall and was due to an issue where the interrupts were not being properly cleared on the interfaces.

- 51190—DHCP clients were not able to receive IP addresses from the firewall in a DHCP relay configuration in cases where the client sent the request in unicast, but could only accept a broadcast reply. Update made to prevent the firewall from modifying the broadcast bit in the client messages it relays to the DHCP server.

- 51171—A VM-100 transmitted a SIP registration packet with invalid IP/UDP checksum values.

- 51107—DHCP Relays were not working when enabled on more than one subinterface.

- 51102—A DHCP client was not able to receive IP addresses through a tagged VLAN port.

- 50994—Importing a custom response page onto Panorama (running on an M-100 appliance) was causing the management server to stop responding upon commit.

- 50959—When creating a custom report using the web interface, the generated final report did not display the columns selected when the report was created.

- 50908—An XSS malfunction occurred when unsanitized input was sent to the Palo Alto Networks next-generation firewall API browser.

- 50891— Executing the command `request system external-list refresh name <name>` in the CLI was causing the refresh request to be shown as coming from the untrust interface, rather than the management interface. This was due to the service route for URL updates being configured to use the untrust interface. This issue only existed when the command was executed in CLI; the corresponding functionality in the web interface worked correctly.

- 50881—The dataplane on a PA-2020 running 5.0.4 became unresponsive after disabling tunnel monitoring on several IPSec tunnels. The issue was due to a race condition that occurred during the commit to disable tunnel monitoring and the existing tunnel monitoring keep-alive messages that were still being sent through the tunnels. Update made to not send the keep-alive messages during a commit.

- 50856—On the M-100 appliance in Distributed Log Collection architecture, a slight difference was noticed between the disk capacity available on the RAID disks and the available capacity identified in memory. This issue caused the M-100 appliance to exceed the maximum log storage quota allotted, and in some cases resulted in the disk becoming full.

- 50814—When an SFP was attached to a port that was in a powered-down state, the media was not detected and the link state was reported as down.

- 50805—Fixed the failure to import and refresh a dynamic block list that was pushed from Panorama to the managed device(s). With this fix, the dynamic block list can be viewed on the device CLI.

- 50802—On Panorama when creating a shared gateway using templates, the ability to assign an available interface to a shared gateway has been added.

- 50657—Fixed a path monitoring issue on the VM-Series firewall that caused flapping in the high availability (HA) state until one device was placed in a suspended state.

- 50640—Fixed the issue with scheduled reports (PDF) being blank when sent an as email attachment from Panorama.

- 50622—Resolved a security policy mismatch that occurred because the group mapping information was intermittently unavailable on the User-ID agent.

- 50614—Addressed the commit failures on Panorama that were caused because old custom reports were not being automatically removed. With this fix, the oldest reports are cleaned up to ensure that adequate disk space is always available.

- 50609—Fixed an exception that caused a dataplane restart when a timing condition error occurred on a neighbor discovery request for a packet.

- 50603—If an appliance enabled for multiple virtual system capability was configured to use a User-ID proxy on one virtual system, while another virtual system was configured to access the LDAP server for group mappings, the group mapping information was not accessible because the User-ID proxy from one virtual system was being used for group mappings on the other.

- 50534—Resolved a connectivity issue on the VM-Series firewall that occurred after a scheduled content update was performed.

- 50519—Fixed a system log error that was generated erroneously to notify that the minimum log retention time was reached. With this fix, the default value for minimum log retention time is reduced from 30 days to 0 days.

- 50518—Fixed the connectivity issue that occurred on a link aggregated interface of a PA-2000 Series appliance, each time a change was committed on the appliance.

- 50495—When FTP was used to download content, and a file blocking profile was used in policy, the flow of traffic recorded in the logs varied by whether passive or active FTP was used. With this fix, the logs are recorded in the direction of the file transfer regardless of FTP mode.

- 50484— When manually running a traffic report to show traffic from a specific subnet the report looked good, but when the report was scheduled and sent using email, data from other subnets also appeared, so the reports were not identical. The issue was due to a problem with the scheduled report not running the query portion of the report that defined the source network that should be reported on.

- 50448—When a dynamic block list was used in a security policy, the dynamic list addresses were intermittently showing 0.0.0.0 soon after a local commit was performed. This caused issues with policy match for addresses defined in the external block list.

- 50444—With several threat prevention features, such as antivirus, if the same host downloaded the same virus from the same server multiple times at intervals more than five seconds apart, the threat log only showed the first download and did not show the subsequent downloads. This also occurred with file blocking and data filtering.

- 50429—When configuring a Panorama device group and a virtual system on a managed device is assigned as the master device for the group, the setting could not be saved if the combined hostname and virtual system name exceeds 31 characters, which is the field limit. This was due to the fact that the hostname of the device and virtual system name was combined when populating the master device field. The maximum hostname length for this field has been increased to 64 characters to accommodate longer names.

- 50408—Security policies were not being applied to traffic going through a virtual wire interface on the firewall when IPv6 firewalling was enabled. This occurred intermittently after a PAN-OS upgrade or a reboot and was caused by an issue where the network prefix for the IPv6 source and destination addresses were using a 32-bit prefix instead of a 64-bit prefix.

- 50392—When migrating the URL Filtering database from BrightCloud to PAN-DB, a commit error occurred. Issue was caused by the fact that the URL vendor migration process failed to delete the BrightCloud update schedule configuration when migrating to PAN-DB.

- 50306—In an active/passive high availability (HA) configuration with the HA2 port configured using a data port in virtual wire mode and then connected to a switch for peer-to-peer communication, the passive device was not sending ARP requests to refresh the MAC table on the switch. This caused the switch to flood when trying to find the HA2 port on the passive device. Update made to have the HA2 interface on the passive device periodically send gratuitous ARP requests to ensure that the MAC table stays up to date.

- 50170—When an HTTP and SSL proxy server was configured between the firewall and the Internet and decryption was enabled on the firewall, clients on the internal side of the firewall that accessed websites through the proxy were not being decrypted. This occurred when the given website used a certificate that was not supported by the Palo Alto Networks next-generation firewall decryption feature. When this occurred, the site should have been added to the decryption exclude cache, but instead, the proxy server was added. This caused other sessions to fail decrypted because the proxy was in the exclude cache. Update made to ensure that the hostname of sites that do not have a supported certificate will be added to the exclude cache, not the proxy server that the clients are using.

- 50133—When configuring a GlobalProtect portal and adding an external gateway address for GlobalProtect clients, the IP format ip-address:port and ip-address/subnet mask could not be added. Update made to allow these formats.

- 50130—When running the command `request system external-list show name` to view the contents of an imported dynamic block list, not all IP addresses in the list were displayed. This was a cosmetic issue only and all items in the list were

adhering to the defined security policy. The issue was due to a buffer limit on this show command, which is now removed.

- 50094—When creating a shared HIP profile configuration using a Panorama template to be pushed to a device group and then attempting to add a HIP notification for the profile, the HIP profile did not appear in the drop-down, so the HIP notification could not be applied. The issue only occurred when doing this from Panorama.

- 50087—Could not delete a Panorama Post Rule tag using the CLI when the same tag was also used in a Pre Rule. This occurred when the rules were part of the same device group. Update made to allow deletion in this scenario because there is no direct dependency.

- 50059—When adding more than 255 terminal services agents to a PA-2020 firewall, a commit error occurred stating that the maximum number of agents was exceeded. Update made to support up to 400 terminal services agents for PA-200, PA-500, PA-2000 Series, PA-3000 Series, and PA-4000 Series devices. On the PA-5000 Series, up to 1000 terminal services agents are supported.

- 50051—The PPPoE encapsulation function was not calculating the payload length correctly for packets sourced from a PPPoE interface. This most often happened on SYN-ACK, FIN, and RST (short TCP) packets.

- 49986—The link speed and duplex settings for the dedicated high availability (HA) interface on the firewall were defaulting to auto-negotiate although configured to use a specific speed and duplex value. With this fix, the dedicated HA interfaces now maintain the link speed and duplex settings defined for the interfaces.

- 49894— When the next-hops of the routes from a dynamic routing protocol changed frequently, it caused the forwarding information base on the dataplane to be updated frequently. This behavior occasionally caused the dataplane to restart.

- 49849— In configurations where captive policy rules were configured to exclude specific source addresses, the clients with the specified addresses were still being prompted to authenticate.

- 49804— When an active/active pair was configured with a destination NAT with active-active-device-binding configured, destination NAT worked correctly. If the active/active pair was converted to active/passive, the destination NAT policy with the active-active-device-binding was not honored

- 49777— When a configuration was triggered to perform a commit by a means other than using the **Commit** button, the start time of the IPSec tunnel was updated, which caused the IPSec tunnel to not re-key before it expired.

- 49749— The firewall continued to use an http request proxy for BrightCloud update after the proxy setting was removed.

- 49748— A captive portal user lost IP to user mapping which caused a default deny rule to be hit. This caused the user to be blocked from services that they should have access to.

- 49578— When network connectivity was removed to the Panorama instance on an M-100 appliance in the active state, it did not cause the Panorama instance on an M-100 appliance in the passive state to move to the active state.

- 49047— An unexpected software reload occurred on a PA-5050 firewall while running in TAP mode because the PAN-DB did not correctly handle some very long URLs.

- 48660— There was a long time lag between when a log message was generated on a firewall and when the log message was received by Panorama. This was due to an increasing time drift caused by the addition of the latency value to the logging rate.

- 48371— Traffic logs for VPN-related traffic, other than from ping, displayed that “0” bytes were sent. This only occurred in traffic logs from PA-5000 Series firewalls.

- 47619— A user failed to log in to a firewall that was authenticated from a Radius server via the CLI using a One Time Password (OTP). This occurred even though logging in via the web interface succeeded.

- 46826— After upgrading PAN-OS software in a high availability (HA) active/passive configuration, the active firewall was unable to obtain the version information from the passive peer. This was occurring even though the passive firewall was able to determine the OS version of the active firewall.

Addressed Issues 5.0.5

- 50608—After upgrading from Panorama 4.1 to Panorama 5.0.4, Panorama commits were failing in configurations that included client certificate profiles because the profiles were not migrated properly in the upgrade.

- 50489—Panorama Template commit locks taken by an administrative user were preventing all subsequent Template commits by any user, including the administrator who took the lock, to fail.

- 50395—Enhanced the authentication functionality to allow the firewall to send only the username and password to the authentication server without the domain name appended even when a domain name is specified in the associated server profile. This allows for proper interaction with authentication servers that do not expect domain names while preserving the proper user- and group-based security policy enforcement

on the firewall. To disable sending the domain name in the authentication response, run the following operational commands on the firewall: `debug authd use-domain no`. By default, the firewall appends the domain name to the username in the authentication response if the domain is specified in the server profile.

- 50335—After upgrading to 5.0.4, PA-5050 devices in active-active high availability configurations were experiencing frequent dataplane restarts due to an internal buffer overflow.

- 50280—DHCP debug logging was enabled by default, causing a larger than expected number of log entries.

- 50271—In active-passive high availability configurations with encryption enabled on HA1, the active device went into a suspended state during the replacement of a peer device. This was occurring because when the active device was unable to connect to the peer over HA1, the high availability agent connected to itself, causing it to detect a device serial number match.

- 50189—Fixed a dataplane restart issue that occurred when jumbo frames were enabled and the packets received buffer was high.

- 50153—Internal path monitoring errors were causing the dataplane to restart. A workaround is to disable internal path monitoring using the following commands: `set system setting packet-descriptor-monitor enable no` and `set system setting packet-path-test enable no`. Problem could not be reproduced, so an update has been made to provide further debug information to help troubleshoot the issue if it occurs again.

- 50136—On devices with multiple dataplanes, UDP traffic was sometimes failing to pass through the firewall in cases where the session had aged out on one dataplane, but the other dataplane did not receive the message to tear down the session. This would cause subsequent sessions to fail, because one dataplane thought it was an active session, but the other one no longer had a session for it. The default time out value has been lowered to ensure that the teardown messages are received on the other dataplane.

- 50092—Out-of-order TCP packets were being dropped when passing through multiple virtual systems on a firewall due to an error calculating the sequence number.

- 49939—The FQDN settings in a security policy were being reset during dynamic block list updates in security policies that contained both an FQDN object and a dynamic block list object.

- 49863—Under very high load conditions in the lab simulated by traffic generators, the PA-3000 Series device would intermittently bypass Layer 7 profiles, such as file blocking and AV.

- 49845—When DHCPv6 relay was configured on an interface that was not using the default virtual router, the firewall would receive the solicit requests from the client, but fail to generate a DHCPv6 relay forward packet to send to the DHCPv6 server.

- 49829—When using the BrightCloud URL filtering database on VM-Series firewalls, URL categories that were configured to be excluded from decryption were still being decrypted.

- 49724—Users were experiencing delays connecting to video conferencing applications because the firewall was initially classifying the traffic as unknown-udp and discarding it. This issue was due to an error creating RTP/RTCP predict sessions in cases where the application only announced one of the protocols.

- 49681—The `test security-policy-match` command was ignoring the `source-user` argument, resulting in misleading results in cases where the IP address to username mapping changed.

- 49567—A firewall in a high availability (HA) configuration performed an unexpected software reload due to memory allocation problems. Dataplane memory utilization has been enhanced to minimize potential destabilizing behavior.

- 49467—Client was unable to pass traffic through the firewall when connecting to GlobalProtect over an SSL-VPN tunnel. This defect only affected VM-Series firewalls.

- 49463—When the license on a VM-Series firewall was refreshed from Panorama (**Panorama > Device Deployment > License** tab), a system reboot was triggered. This issue is now resolved, and a system reboot occurs only when Panorama detects a change in the capacity license applied to the VM-Series firewall.

- 49416—RSH sessions passing through a firewall were halted when multiple RSH commands were run within a short period of time. Content update 370-4630 or later is required for this bug fix.

- 49343—Web sites were loading too slowly for traffic passing through the firewall due to a missing BrightCloud license, which slowed the URL resolution process.

- 49337—Traffic was blocked even though the DoS Protection policy was configured to allow it.

- 49288—After the management interface was changed from the default on the firewall and the change was committed, access to the firewall was available from both the new address and the default address after the system was restarted.

- 49201—Panorama failed to import log files from the firewall.

- 49171—Access to the Palo Alto Networks next-generation firewall web interface was not available from Internet Explorer 7.

- 49143—When updating the content version on a firewall, “unknown-tcp” traffic was logged for a few seconds.

- 49114—Customer was unable to add User-IP Mapping to a firewall using the API and the following error message was displayed: “User not authorized to perform this operation”. This problem occurred with an admin account created with the “User-ID Agent” privilege only. The issue has been resolved with this release.

- 49076—In a high availability (HA) pair with “heartbeat backup” configured one firewall was rebooted. The firewall being rebooted experienced repeated software reloads while receiving “heartbeat backup” messages from the other firewall in the HA pair. The issue has been resolved with this release.

- 49075—Some DoS policy CLI commands were not taking affect or showing expected output. The issue has been resolved with this release.

- 49012—The firewall stopped logging because the log partition was filled with packet capture (pcap) files. The issue has been resolved with this release.

- 48985—Addressed a system restart that was caused by a loop and generated a missed heartbeats syslog message.

- 48929—When using Panorama to manage the PA-3000 Series firewall, the **Panorama > Device Deployment > Licenses** tab displayed the PAN-DB URL Filtering license as invalid.

- 48927—On importing a configuration file after upgrading Panorama from 4.1 to 5.0, the web interface did not display the certificates. This issue is now addressed, and the certificates display.

- 48897—Added license expiration notification in the system logs for PAN-DB URL Filtering and WildFire subscriptions.

- 48874—When using RADIUS Vendor Specific Attributes (VSAs) on Panorama for managing administrative access to the firewalls, CLI access was denied to administrators enabled for CLI access. This issue is now addressed.

- 48870—Addressed a failure to recognize a CA certificate as a Trusted Root CA when the Path Length Constraint was defined on the certificate.

- 48864—Fixed the inability to download and install content updates from the active Panorama peer to the passive peer in a high availability (HA) configuration using the 'Sync to HA Peer' option.

- 48829—On a firewall enabled with multiple virtual system functionality, a custom threat signature name created on virtual system1 was displaying in the threat logs on virtual system2. This issue has been addressed and the threat logs only display in the virtual system that includes the custom signature.

- 48708—Fixed a restart that occurred on a firewall that was configured as a captive portal.

- 48672—Fixed an issue on the PA-200 and the VM-Series firewall that caused a temporary failure to detect an infected file (with an antivirus security profile enabled) after a configuration change was made to any security policy rule.

- 48639—Addressed an issue with enabling a dynamic DHCP client on an external interface using an IPv6 address with a NAT64 translator.

- 48555—Resolved an error that occurred when pushing template changes from Panorama to a managed device.

- 48499—In an active/active high availability configuration, the DNS proxy failed to resolve hostnames when configured with a floating IP address.

- 48497—Environments with a large number of NAT DIP/DIPP rules may experience an error condition committing or upgrading to PAN-OS 5.0: Error updating NAT IP pools failed to handle CONFIG_UPDATE_START. To help you reconfigure NAT rules to use less memory, information about memory usage has been added to the `show running nat-rule-ippool` CLI command showing NAT rule memory usage by virtual systems. You can either delete unnecessary NAT rules or compress NAT rules to reduce memory utilization. For example, you could compress DIPP NAT translation from a /27 address range to a /32 IP address.

- 48443—The agentless User-ID lost the user to IP address mappings, which caused a miss in matching policy based on users/groups therefore causing the default policy to be applied to all users. This issue has been fixed.

- 48411—User-ID was not able to retrieve directory group names if the group name contained a comma followed by a space. Issue was due to a problem with the short name conversion process of the group attributes when this character combination was present in the group name.

- 48156—Intermittent split-brain issue occurred on a PA-2050 high availability (HA) active/passive configuration due to failures with the flow management process. Issue was not reproducible, so additional debug code has been added to help troubleshoot the issue if it occurs again.

- 48151—This bug fix addresses two issues. The first issue is that Panorama received the error **Configuration is invalid** when trying to commit a configuration that contained more than 2048 FQDN address objects. Although 2048 is the limit for firewalls,

Panorama should not have failed the commit. The second issue was that PAN-OS had an FQDN address object counting issue where if the same object existed in multiple virtual systems, the object was counted multiple times. Update made to only count the address object once if the same object existed in multiple virtual systems.

- 48143—The routed process stopped responding multiple times on the passive device in an active/passive high availability (HA) configuration when large amounts multicast traffic was being processed by the HA pair.

- 48130—When the **SSL Inbound Inspection** option was configured in a decryption policy rule, the **Decrypted** check box was not checked when viewing the session in the traffic log details view.

- 48103—The syslog format for threat and traffic logs changed in PAN-OS release 5.0, which caused issues with certain syslog servers. Issue due to a problem where a NAT rule was in place for a specific destination address, but other addresses that did not require a NAT resulted in an empty value. Update made to produce the value 0.0.0.0 for these addresses, which was the previous behavior.

- 48041—When configuring a service route for SNMP Traps to use a configured L3 interface, the commit failed unless a destination address was entered. The destination address should not have been required for this configuration.

- 47906—Dataplane on a PA-5000 Series device was intermittently restarting due to an egress output buffer overrun issue.

- 47844—Logs were being generated for the internal dns-proxy object, even when DNS proxy was not enabled on the firewall. This was normal behavior and the log was generated when FQDN resolution was required in address objects. Logging for this event has been removed because it is not something that the firewall administrator needs to monitor.

- 47703—The firewall was increasing the Maximum Segment Size (MSS) value sent by a host on the trust side to a host on the untrust side during the TCP handshake. This caused issues with the receiving servers on the untrust side, which caused packets to be dropped. Update made in this release to set the MSS sent to the client to the interface's MTU minus headers if the "Adjust MSS" option is set on the ingress interface.

- 47589—Traffic stopped passing after a high availability (HA) failover and fallback with the preemptive option configured. The issue was intermittent and was due to a problem with Forwarding Information Base (FIB) entries not being updated properly.

- 46721—Dataplane on the firewall intermittently stopped responding when decryption was configured. Issue was due to packets becoming out of order during the decryption process.

- 46705—PA-5000 Series firewall in virtual wire mode was causing multicast traffic to become out of sync and duplication was occurring during session setup, which caused packet drops.

- 45903—When using App Scope to view the top 5 threats for the last 24 hours, the error "Your session has expired" occurred. Issue due to a problem where a single quote in a threat name caused a rendering issue with the report chart.

- 37315—When a firewall was configured with Kerberos authentication and an authentication request was received, queries to domain servers other than the server defined in the Kerberos server profile occurred. Update made to ensure that requests are only sent to the server(s) defined in the **Device > Server Profiles > Kerberos** list.

Addressed Issues 5.0.4

- 49315—After upgrading to content version 362-1714 or later, which includes new BrightCloud categories, attempts to view the URL filtering logs caused the management server to restart.

- 49275—Dataplane intermittently restarting on PA-3000 Series devices. Issue isolated to this platform and has been resolved in PAN-OS 5.0.4.

- 49084—When setting a commit lock on a Panorama device group and then removing the commit lock, the administrator could not commit the configuration and received an error stating that the commit lock was still in place. The issue was due to a problem releasing commit locks on device groups.

- 49061—When using a traffic generation tool with a particular traffic pattern, the PA-5060 was not able to reach the maximum TCP sessions allowed by the firewall when App-ID was enabled. When Application override was enabled, the device performed to specification. Update made to increase session capacity when App-ID is enabled.

- 49048—The zone names in traffic logs were being truncated for virtual systems logs when the VSYS ID contained two or more digits.

- 48975—High availability (HA) failover was occurring when the PAN-DB URL filtering feature was enabled and the administrator selected **Request categorization Change** in the URL Filtering log detailed view. The issue occurred when the admin selected a category from the drop-down that did not exist in the BrightCloud category list. The issue was due to a problem where the category list was not properly updated after a PAN-OS upgrade. An update was made to reset the URL categories back to the default list if the suggested category does not exist in BrightCloud.

- 48966—Files could not be uploaded to the firewall using cURL with the XML API. Using wget worked fine. Update made to fix the cURL issue.

- 48817—Fixed an issue that occurred with the Content-ID engine when the firewall was under extreme load.

- 48797—The PAN-OS User Mapping (agentless User-ID) was not able to communicate with the Active Directory (AD) domain controller if the DNS response returned during a discovery had the truncated flag set.

- 48688—When configuring a policy that had both addresses and regions and the policy used the negate option (option to choose any address except the configured ones), the policy did not work properly. Issue due to the PAN-OS code not properly honoring De Morgan's law, which is a set of rules that determine inclusion/exclusion principles. This bug also addressed a cosmetic issue where the command `show running *-policy` displayed `any` for policies with no addresses or regions when it should have displayed `none`. For example, `show running security-policy` on a policy that does not have a region displayed `any` for the `destination-region` when it should have displayed `none`.

- 48612—User activity reports with a custom time period configured showed the following error instead of the user data: `Error parsing xml…` Issue due to a problem with the report engine reading in the custom date/time format.

- 48601—Some sessions were being closed during a commit after a zone was deleted from one of the virtual systems in a multi-VSYS configuration. The issue occurred in a multi-VSYS configuration with a shared gateway configured. When a zone in one virtual system was deleted, this impacted sessions for clients in other virtual systems because the shared gateway was reset when the zone deletion was committed.

- 48521—Destination and static NAT rules failed after upgrading from PAN-OS 4.1.x to PAN-OS 5.0.x. Issue due to IPv6 firewalling being enabled by default in 5.0, which caused searches to be done using addresses formatted for IPv4 against rules formatted with IPv6. Disabling IPv6 firewalling fixed the issue and after re-enabling, the issue no longer occurred. Issued resolved and disabling and re-enabling IPv6 firewalling is no longer necessary.

- 48497—Environments with a large number of NAT DIP/DIPP rules may experience an error condition committing or upgrading to PAN-OS 5.0: `Error updating NAT IP pools failed to handle CONFIG_UPDATE_START`. To help you reconfigure NAT rules to use less memory, information about memory usage has been added to the `show running nat-policy` CLI command showing NAT rule memory usage by virtual systems. You can either delete unnecessary NAT rules or compress NAT rules to reduce memory utilization. For example, you could compress DIPP NAT translation from a /27 address range to a /32 IP address.

- 48491—When scheduling dynamic updates for WildFire signatures and also scheduling a threshold for the Applications and Threats update schedules, a delay occurred when the device attempted to download WildFire signatures. For example, when WildFire was scheduled to update every 15 minutes and the Applications and Threats schedule had a threshold of 12 hours, WildFire did not update if the WildFire signature was less than 12 hours old. An update has been made to stop WildFire signature updates from being tied to the Applications and Threats threshold setting.

- 48481—When viewing security policies on a multi-VSYS firewall, hovering your mouse to the right of the policy name and choosing Log Viewer took you to the monitor logs traffic page. This should take you to the logs for the virtual system that you were viewing, but instead it showed Virtual System All.

- 48476—The firewall restarted when reading corrupted log files. The log indexing process has been changed to skip reading log files that have been corrupted.

- 48453—The firewall restarted because a null high availability (HA) message was received in an HA packet from an HA peer. This issue has been resolved by allowing the firewall to receive a null HA message gracefully and increment a global counter.

- 48378—Fixed a dataplane restart. This restart occurred when some interfaces were operating in L2 mode, and the packet buffer was running low on a system under heavy load.

- 48272—When querying for the policy rule that matched a threat name or CVE in a vulnerability profile, the rule name was not displayed in the query results. This issue is now resolved.

- 48260—Fixed a forwarding issue on the PA-5000 Series firewalls that caused out-of-order packets and an intermittent loss of UDP packets, in an active/active high availability deployment.

- 48195—On the PA-3000 Series, when system resources such as CPU were under high utilization, the action defined in the security profiles were sometimes disregarded. With this fix, when a system resource is overloaded, the session will be dropped.

- 48047—When upgrading a device from PAN-OS v 4.1.6 to 5.0, the upgrade would fail and the device would reboot. This issue was seen if the configuration included invalid IP address formats or if a certificate parsing error occurred when a newline was not used to separate multiple certificates. This issue is fixed.

- 47990—Fixed the issue that caused an SSH connection failure when an aggregated Ethernet interface and a VLAN interface were attached to the same physical interface.

- 47951—The firewall restarted during a de-schedule operation when a packet was put into an IPSec tunnel and routed to another virtual system. The packet was fragmented after being encapsulated into the tunnel and a new packet was allocated. The firewall was restarted because the new packet did not match the packet in the queue.

- 47920—When configuring firewalls managed by Panorama to forward logs to an M-100 log collector, instead of to Panorama, some firewalls did not get the preference list updates that instruct the firewall on where to send logs. The issue was due to a problem sending the preference list to device groups that contained more than 19 firewalls. Checks put in place to ensure that the preference list will be properly sent to the managed firewalls.

- 47896—Fixed an application timeout that occurred because the custom timeout setting configured for the application was disregarded.

- 47890—The firewall performed frequent restarts when the ICMP TTL expired.

- 47832—On a PA-5000 Series device, the sysd process sometimes experienced a virtual memory space spike to above 2GB. When this occurred, the overall system performance sometimes deteriorated and eventually impaired traffic processing. This issue has been addressed in this release by not triggering the virtual memory space spike in the sysd process.

- 47826—Panorama would successfully push a WildFire content update to a managed device that did not have a WildFire license. This issue is now resolved; you can use Panorama to push WildFire content updates only to managed devices that have a valid WildFire license. Panorama will report the failure to update the content database on a device without a WildFire license.

- 47647—Improved the response time on the Panorama web interfaces; the time to load the reports or logs on the ACC is significantly faster.

- 47581—Fixed the buffering issue that caused the firewall to stop forwarding traffic when a large number of UDP streams were sent over a GlobalProtect tunnel enabled for SSL VPN traffic.

- 47540—In a captive portal without NAT configured, the idle timeout as displayed in output from the `show user ip-user-mapping` command, was incorrectly refreshed by traffic coming "to" the captive portal user IP address. With this release a refresh only occurs when traffic is generated "from" the IP address.

- 47529—The firewall traffic logs displayed an IP address range in the country name column. Issue has been resolved with this release.

- 47506—On a PA-4000 or PA-5000 Series device, packets to the L2 interface were sometimes forwarded back out the same interface intermittently. This incorrect Layer 2 behavior could confuse the switch connecting to the device and cause MAC forward table flapping.

- 47323—NetFlow packets were sent with an InputInt value of 0 from a VLAN configured on a firewall, which caused them to be dropped by a NetFlow collector.

- 47285—After Unidirectional Link Detection (UDLD) on a connected switch brought down a port on the firewall, the port did not come up when the port returned to the active state on the switch. Issue has been resolved with this release.

- 47217—Command line interface would not accept input in languages that use a 2-byte character set such as Japanese or Chinese in UTF-8. Issue has been resolved with this release.

- 47161—Only one zone protection log is created when alarms were generated from multiple virtual systems.

- 46835—Fixed a restart issue that was triggered by a memory consumption increase in the User-ID process. This issue was noted when the devices were in a high availability configuration and the devices received a large number of HIP reports.

- 46728—A Tech Support file generated on the firewall could be downloaded without the admin being prompted for user authentication. The issue is now fixed; to download the Tech Support file the admin must log in using a valid username and password.

- 46649—When denying a web session with a response page, the firewall did not perform a proper close for the TCP connection, causing the client to remain half-open.

- 46510—The DNS server was not used by the management interface in a DNS proxy configuration where the DNS server is inherited and the DNS proxy object is used for management.

- 46364—The firewall experiences Radius authentication failures when running in FIPS/CC mode.

- 45687—When high availability (HA) fails over from the active device to the passive one, it takes more than a couple of minutes to re-establish the OSPF adjacency when the OSPF database is large. This issue is rare. It is due to the new active device sending redundant Database Description (DD) packets. If the neighbor OSPF router cannot handle the duplicate OSPF DD packets, the OSPF database exchange can be aborted multiple times. This issue has been resolved with this release such that the redundant DD packets are not sent.

- 45649—When using the Classified option in a DoS profile and then applying that profile to a DoS policy, threat logs were not generated when the Alarm rate was exceeded. Update made to properly handle the Classified option.

- 44952—When a Copper SFP was configured in forced mode and the cable was removed, the LOS signal was not transmitted to the switch. Because the LOS signal was not transmitted, the link failure was not detected.

- 44844—Intermittent failures occurred when connecting a firewall using LDAP over SSL (LDAPS) to a server.

- 43247—The following message was generated when performing PCI checks on the external interface of a firewall: "This system is running a web application that does not set the 'secure' attribute for session cookies established over secure (HTTPS) connections. A browser subsequently requesting the same site over a non-secure (HTTP) connection may send the cookie in clear text. An attacker could exploit this to obtain the cookie and hijack the users session".

- 42331—When exporting a custom PDF report, the IP address for a source or destination was not being resolved to its hostname. Now, the exported PDF maps the IP address to the hostname, and the report displays the hostname accurately.

Addressed Issues 5.0.3

- 34611—After committing the configuration on a firewall, all QoS historical data is cleared. However, the QoS bandwidth graphs were showing a negative value instead of showing zero after a commit. Update made to correct the negative value issue.

- 38325—Commit was failing to continue after reaching the 98% mark and was waiting for SSL VPN to respond. Workaround is to restart the sslvpn-web-server. Problem could not be reproduced, so an update has been made to provide further debug information to help troubleshoot the issue if it occurs again.

- 38781—Commit issues were occurring when trying to enable DHCP relay using the CLI when the IP address was set, but the enable option was not set to yes. The CLI also allowed the enable option to be deleted, which caused a problem in the configuration. Additionally, the web interface would show that the DHCP relay was enabled even when it wasn’t.

- 41353—AV updates were triggering a full retrieval of the group mappings and, during the buffering process, group names using double-byte character sets were being inadvertently encoded and added to the Group Include List improperly. As a result, policy was not being enforced properly for members of the affected groups because the group name on the Group Include List no longer matched the actual group name.

- 42147—PPPoE sessions were failing on the firewall when a PPPoE relay device was used between the firewall and the PPPoE sever. Issue due to a problem where the firewall was not parsing relay session IDs that begin with Null. As of this release (5.0.3), PAN-OS will now work with PPPoE relay.

- 42331—When exporting a custom PDF report, the IP address for a source or destination was not being resolved to its hostname. Now, the exported PDF maps the IP address to the hostname, and the report displays the hostname accurately.

- 42576—Performance issues observed when using a traffic generator to send traffic through Layer 2 interfaces on PA-500, PA-2000, and PA-3000 devices. Issue was caused by a problem with how MAC address updates were being handled on these models.

- 43831—Resolved the failure to obtain an IP address for an interface when using a DHCP client.

- 43970—Firewalls with multiple dataplanes were aging out FTP sessions when large file transfers traversed the firewall. Issue due to a problem where refresh failed to propagate between dataplanes causing session aging and a tear down of the mirror sessions on the other dataplane.

- 45139—Custom reports that did not have the schedule check box checked, were running with other scheduled reports. Issue due to a problem where reports that were part of a report group that had other reports that were scheduled caused the non-scheduled reports to run as well. Update made to filter out the non-scheduled reports.

- 45313—Resolved a dataplane restart that occurred when SSL decryption was triggered on a security rule with a file blocking profile.

- 45422—Firewall stopped forwarding traffic on one occasion, possibly due to a memory issue created by an IP parsing problem with address objects. In this case, it was observed that addresses with the slash notation were not interpreted properly and the last octet was zeroed out. For example, 192.168.2.50/24 was interpreted as 192.168.2.0/5024.

- 45492—When an LDAP domain was defined on the firewall for user to IP mapping purposes and the NETBIOS name was entered in upper case, reporting problems occurred for users in that domain. This was noticed in a custom URL report and no user data was populated. If the domain was left empty or was in lower case, the same reports were fine. Update made to determine the correct domain name if it is in upper or lower case.

- 45784—Users authenticating to GlobalProtect using AD were getting notified that their passwords were going to expire in x number of days, even though a Group Policy Object specified a maximum password age of 0 (which means passwords do not expire). Previous work around required individual accounts to be set with the Password never expires option turned on. Issue due to a problem with AD Authentication profile not recognizing the maximum password age setting of 0.

- 45807—Although configured by policy, for SSL web content the browser did not display the block or continue page to the user. This issue is now fixed.

- 45945—Some DHCP clients (mainly Apple devices) were not able to receive an IP address from the firewall when DHCP relay was configured. Issue was due to a problem where the DHCP clients expected a unicast reply from the firewall, but the firewall was sending a broadcast. Problem may have also been attributed to the fact that the clients were on a very large broadcast domain. Update made to have the firewall relay a unicast to the client when the DHCP server replies with unicast in the packet's broadcast bit.

- 46031—This fix addresses an issue where each call for a time stamp did a time zone check by accessing a file on the system's hard drive. For example, each time a time stamp was needed to record the session start time for a traffic log, the process would check the time zone file on the hard drive. This was not optimal for performance, so this change only requires the system to periodically check the time zone.

- 46197—In an active/active high availability (HA) configuration with virtual wire interfaces, traffic was not being processed properly. This issue is now resolved and the traffic flow is effectively managed on the firewall.

- 46306—TCP packets were intermittently being re-ordered when they went through the firewall over a virtual wire. The issue caused problems with an external print server because the two hosts could not establish a proper handshake. Previous to this release, if an app override rule existed for a session, the session was not offloaded until after the first data packet. This caused a race condition and a re-ordering of packets when a FIN was received while the data packet was being processed by another PAN-OS task. The update made in this release will turn off the App-ID task that caused this issue on the final ACK of the 3-way handshake if PAN-OS determines the application for the session and there is no decoder for the protocol.

- 46367—Performing an AV update directly after a Validate candidate configuration operation was causing the temporary candidate configuration files to be written to the running configuration. The next time the configuration was reloaded (commit, content update, or restart), the candidate configuration would then become the running configuration.

- 46429—Dataplane intermittently restarted on PA-4000 Series devices due to packet buffer issues. Problem could not be reproduced, so an update has been made to provide further debug information to help troubleshoot the issue if it occurs again.

- 46470—The configuration lock was not showing that the configuration was locked until an administrator attempted to commit changes to an area of the configuration that was locked by another administrator (rather than showing a message indicating that there was a lock at the time the administrator attempted to make a change). The issue was due to a problem that occurred when a system was in multi-VSYS mode and was then changed back to single VSYS, the single VSYS was defined as shared instead of VSYS1.

- 46500—Mprelay, a process that communicates between the dataplane and the management plane, was crashing after a commit when PBF configuration changes were made.

- 46502—When viewing the Change Monitor report from the **Monitor > App Scope** page and clicking one of the line points in the chart to open the corresponding ACC view, the time field located directly under the ACC tab would show the incorrect time. For example, if at 4 P.M. you were looking at the Change Monitor for the last 24 hours and then clicked a point on the line char, the ACC time field would have shown a range of 4 A.M. from the day before to 4 A.M. of the current day, when it should have instead shown 4 P.M. of the current day.

- 46507—The snmpd.log file was being frequently cleared because of a log overflow that was caused by repetitive logging of invalid messages. The issue is addressed and invalid messages are no longer written to the log file.

- 46564—Importing a .p12 certificate to the firewall failed with the error "Import of certificate and private-key certname.local failed. Validity period cannot be more than 30 years." Update made to remove validity period check when importing certificates.

- 46585—In an active/active configuration, Captive Portal was failing with Internet Explorer versions 7 and 8.

- 46620—ICMPv6 traffic was failing due to problem where the VLAN tag was being lost in the packet header.

- 46628—When Captive Portal roaming was enabled, users had issues connecting to resources when they moved to a different network and their IP addresses changed. Issue due to a problem recognizing the username after an IP address change.

- 46631—When previewing changes during a commit from Panorama, the interface was not always showing previews for the number of contexts you selected.

- 46647—The management web interface could not be accessed over the IPv6 link local address. We do not specifically prohibit this type of access, though this action is not currently defined in any RFC and not supported by current browsers.

- 46672—On the PA-2020, the high availability (HA) link monitor did not detect a link status change on the SFP port. This issue is fixed.

- 46714—Resolved the failure to display a custom response page for a decrypted SSL session. With this fix, a custom response page displays when a request in an SSL session matches a URL filtering category that is blocked by policy.

- 46820—Resolved a restart that occurred on the firewall when uploading large files to the WildFire public cloud.

- 46823—URL database updates were causing a path monitoring failure, which would then trigger a high availability (HA) failover. This issue is fixed.

- 46835—Fixed a restart issue that was triggered by a memory consumption increase in the User-ID process. This issue was noted when the devices were in a high availability configuration and the devices received a large number of HIP reports.

- 46857—Fixed a possible command injection vulnerability that could occur in the NTLM settings, when configuring the User-ID Agent.

- 46864—Fixed an issue with the policy evaluation process where FTPS traffic was being blocked because the inbound SSL decryption policy rule that allowed the traffic was not being matched properly.

- 46870—GlobalProtect connections were successful with a revoked client certificate. With this fix, when a GlobalProtect client with a revoked certificate attempts to connect to the GlobalProtect gateway, the certificate is not accepted and the user receives a "Client Certificate Error" message.

- 46922—Dynamic update was ignoring the update threshold when a threshold was set for both Applications/Threats and Antivirus. For example, if you set an Application/Threat update to only download updates older than 120 hours and also set a threshold for Antivirus updates, the Application/Threat update would ignore the threshold and would update regardless of the age of the update package.

- 46936—In an active/active high availability (HA) configuration, configuration sync was not occurring automatically and when a manual sync was performed; the HA link started to intermittently lose connectivity. Issue due to a problem where HA1-Backup was incorrectly determined to be down during a commit, but after a few seconds the pings continued and the interface was fine.

- 46975—On Panorama, when you used the ACC to query the managed device for logs, the timestamp for the query was recorded incorrectly. With this fix, the managed device and Panorama display the same timestamp for the requested data.

- 47038—When using SCP to export a configuration from Panorama (**Panorama > Scheduled Configuration Export** tab), you could not insert a SSH host key to complete the export. The issue is now resolved and you can successfully export the configuration file using SCP.

- 47059—The web browser would stop responding after removing the configuration lock and committing a change on Panorama. This issue is fixed.

- 47066—With multicast routing using Protocol Independent Multicast Source Specific Mode (PIM-SSM), only the default 232.0.0.0/8 address was accepted as a valid input. This issue is now resolved and you can now add any other group range for PIM-SSM multicast, for example, 225.10.0.0/16.

- 47082—Fixed a commit error that occurred when the application-default service was dragged in to a security policy rule. This issue is fixed; the drag and drop functionality in the web interface works properly.

- 47094—When using the Panorama web interface, if a configuration lock was taken for a device group that has spaces in the device group name, the lock could not be cleared. This issue is now fixed.

- 47109—Resolved a restart issue that occurred when the HA2 link failed on the active-secondary device in a high availability (HA) pair.

- 47133—Fixed a zone validation failure that occurred because the network zone was incorrectly recorded in the device configuration XML file.

- 47135—The firewall was sending the correct data to the management server, but the MIB file was missing the definitions for PanSeqno and panActionflags data, so third-party SNMP monitor applications could not display the data because it was not interpreted correctly. The corrected MIB files have been fixed and are posted here: https://live.paloaltonetworks.com/docs/DOC-4120

- 47214—Custom traffic and threat reports generated on Panorama displayed the wrong virtual system (VSYS) name for a VSYS ID. This issue is now resolved. Reports generated from the traffic and threat summary table only display the VSYS ID; the VSYS name is displayed only when the device serial number column is also included in the display filter.

- 47222—When a URL with a hex character at a specific location was saved to the URL cache during the categorization process, a dataplane restart occurred.

- 47237—When mapping an IP address to a MAC address for DHCP reservation, the firewall would not normalize the upper case and lower case letters entered for the MAC address format. So, the MAC address aa:aa:aa:aa:aa:aa and aa:aa:aa:aa:aa:AA were each regarded as unique MAC addresses. This issue caused errors and misconfiguration when more than one IP address was reserved for the same MAC address.

- 47241—When changing log quotas on the Panorama **Device > Management > Logging and Reporting Settings** tab, the new values were not taking effect because the device was inadvertently calculating the quotas to be in excess of 100% even when they weren't, therefore discarding the changes.

- 47243—Custom Regional Objects pushed from Panorama were not showing in their respective regions based on latitude(N) and longitude(E) in the web interface on the device because the device was unable to get the aggregate list of regions (predefined + custom + Panorama pushed) from the running configuration.

- 47266—Commits were failing because one of the many daemons that participate in the commit process did not handle commit failures under certain conditions.

- 47308—The VM-Series firewall did not report on interface statistics.

- 47315—After upgrading to 5.0.x, you could no longer successfully commit decryption rules that included both a destination country and a URL category due to changes that were made to accommodate dynamic address objects.

- 47385—On PA-4000 Series devices, asymmetric traffic was experiencing latency issues of approximately 10 microseconds with TCP traffic traversing the firewall that arrived on virtual wire 1 and returned on virtual wire 2. Issue due to a problem where the network processor was not properly handling traffic when the egress information is not the same. This caused the packets to be sent to the main CPU for forwarding instead of directly from the network processor.

- 47387—Administrative user accounts that were locked, for example due to failed login attempts, could not be unlocked from the web interface.

- 47409—OSPF issues occurring after a failover and then a recovery in an active/passive configuration with the Preemptive option set. Issue due to a problem where the passive device changed to active, but the router daemon still received route messages that had a different Route Table Manager (RTM) generation ID. Update made to drop the route messages if the device is already active.

- 47429—The custom report API was failing to generate reports on devices with a single virtual system.

- 47436—Firewall interfaces configured as DHCP clients were unable to communicate with DHCP servers that do not support the broadcast flag. The DHCP client will now attempt to send a unicast request if discovery fails when using a broadcast request.

- 47546—New Active Directory users were not being mapped to their primary groups on the firewall if the primary group was one of the Active Directory built-in groups, such as Domain Users, because the firewall did not recognize that the group had changed and was therefore inadvertently discarding the changes. The group mapping function has been fixed so that it now properly maps additions to the built-in groups.

- 47565—After upgrading to PAN-OS 5.0.x, newly imported certificates that were part of a certificate chain were being stripped of their intermediate certificates, causing the browser to prompt users with a certificate warning.

- 47577—In rare cases, the management plane runs out of memory, triggering a failover. Additional management plane monitoring statistics have been added to help identify and diagnose memory issues.

- 47674—In some cases, modifications to the Captive Portal response pages were causing the web server instance that handles Captive Portal to fail due to internal processing errors.

- 47783—During the upgrade from Panorama 4.1.9 to 5.0.1, the certificate expiration date was not transformed properly, causing device group commit errors.

- 47813—Made a change to disable the use of SSL compression on HTTP-TLS interfaces on the device.

- 47827—When displaying statistics on the **Network > QoS** tab in the web interface, the x-axis was not displaying a time range during the first five minutes of the rendering period. This has been fixed so that the graph initially shows the time range in 15-second intervals, changing to a one-minute scale after the first two minutes of graphing.

- 47849—Users connecting via GlobalProtect were not successfully getting IP address to username mappings in some cases because the SSL VPN was not accepting the HIP report. This issue was due to the fact that the User-ID initial HA MD5 checksum was failing in the case where a HIP report was deleted after a commit, preventing User-ID from notifying the SSL VPN that it was ready to accept HIP reports.

- 47942—In some circumstances, high availability (HA) failover is not being triggered when the active device stops passing traffic. Additional statistics have been added to the Tech Support File to help diagnose hardware issues related to this issue.

- 47948—The User-ID process on the firewall was consuming excessive CPU resources due to improper rate limiting of unknown IP address requests.

- 48044—In the session browser, only client-to-server traffic was counted in total byte count. The issue is resolved to count both client-to-server and server-to-client traffic.

- 48064—On PA-5000 Series and PA-3000 Series devices, the path monitor was taking longer than expected to trigger a failover because the internal firewall processes were not properly resetting the maximum missed heartbeat counter in certain situations.

- 48095—Fixed an issue with internal index generation that was causing latency when managing the device from the web interface and/or the CLI.

- 48124—New DHCP clients were not receiving DHCP addresses from the firewall in a timely manner when requesting an IP address issued previously by a different DHCP server. Issue due to a problem where the Palo Alto Networks next-generation firewall DHCP server was not sending a NAK to the client when the request was received.

- 48193—User names containing double byte characters were not displaying properly in traffic detail logs and exported CSV reports.

- 48218—User groups that contained the special character "&" were displaying with the individual user icon rather than with the group icon in associated security policies.

- 48304—Sub-groups were showing up in User-ID group mappings even though only the parent group was explicitly included in the group mapping configuration.

- 48860—Custom response pages were not displaying in client browsers after PAN-OS upgrade due to improper packet segmentation.

- 48994—TCP sessions that matched an application override policy were being closed after a few seconds and the packets were being dropped because the application override was being invoked too early in the handshake process, causing the TCP timeout to be set too low.

Addressed Issues 5.0.2

- 47280, 46424, 46405, 45635—The User-ID agent on a Windows 2008 server was intermittently failing to respond when the directory contained 50,000+ users, causing valid user to IP mapping information to be deleted on the firewall. This occurred when the session limit of the firewall was being reached. Issue was due to a buffer problem that occurred when trying to write the user to IP mapping to the firewall.

  Updated - To ensure that this bug is fixed in your environment, we recommend you run User-ID agent 5.0.3-4 or later. This version of the User-ID agent is backward compatible with PAN-OS 4.1.x. The recommended PAN-OS version for this issue is 4.1.11-h3 (hotfix 3) and 5.0.4.

- 47195—When the App-ID cache feature was enabled in previous releases (enabled by default), it was possible to pollute the cache to allow some applications to pass through the firewall, even when a rule was set to block the application. If you are running an older version of PAN-OS, you can disable the application cache by running `set deviceconfig setting application cache no` until you can upgrade.

  With this update, the App-ID cache will not be used in security policies by default. The following new CLI command has also been introduced to control whether or not the App-ID cache is used: `set deviceconfig setting application use-cache-for-identification` and is set to **no** by default.

  For more information, please refer to the Security Advisory PAN-SA-2013-0001 at https://securityadvisories.paloaltonetworks.com/.

- 46849, 46844, 46681, 46474—The firewall was intermittently failing to respond to DHCP requests from hosts after upgrading to PAN-OS 5.0. Issue due to a problem that occurred after lease information was saved on the firewall every 12 hours after a restart, the issue was cleared, but would then occur again after 12 hours.

- 46832—Fixed a policy lookup error that occurred when a custom URL category was used to define a URL pattern. With this fix, when performing a policy lookup, the firewall will first evaluate custom categories configured on the device before using the predefined categories included in the URL database.

- 46815—Resolved a restart that occurred on Panorama and the M-100 appliance running v5.0.0 when exporting the configuration logs to the CSV format from the **Monitor > Logs > Configuration** tab.

- 46799—SSL interception was incorrectly occurring on websites that were configured to be exempt from decryption. This error occurred because the common name on the SSL certificate was read inaccurately, thereby causing a mismatch in accurately categorizing the URL and applying policy. This issue is now fixed and the SSL certificate is read accurately and the URL category is matched for accurate policy behavior.

- 46780—QoS bandwidth and runtime statistics did not display in the **Network > QoS** tab. The issue is now addressed and the statistics are displayed for the interfaces configured for QoS.

- 46747—Fixed a log quota error message that was displayed when attempting to upgrade the PAN-OS version from v5.0.0 to v5.0.1. The upgrade process now succeeds without errors.

- 46741—Fixed an issue that enabled modification of the HTTP post arguments to redirect the GlobalProtect portal login URL.

- 46728—A Tech Support file generated on the firewall could be downloaded without the admin being prompted for user authentication. The issue is now fixed, to download the Tech Support file the admin must log in using a valid username and password.

- 46712—The management plane stopped responding when processing abnormal GlobalProtect requests due to an issue verifying user input. Also, the User-ID process failed during HIP rematch when the number of reports exceeded the maximum entries in the HIP cache due to a race condition.

- 46699—The GlobalProtect login page was failing PCI scanning because autocomplete was enabled.

- 46678—Improved validation of user data on the Palo Alto Networks next-generation firewall web interface.

- 46655—Jobs were getting stuck in the pending state when batches of scheduled reports were suspended without successfully resuming.

- 46637—In an active/active high availability (HA) deployment, aggregate Ethernet interfaces were not receiving ARP replies from the virtual MAC address. This issue has been fixed.

- 46547—Fixed a dataplane restart in the URL filtering module after a high availability (HA) failover was triggered.

- 46538—In a high availability (HA) lite configuration on a PA-200 device, if the passive link state was set to auto the device would send empty HELLO messages, causing flapping neighbor adjacencies.

- 46506—Management server intermittently restarted due to a Null point access problem.

- 46504—On PA-4000 Series device running PAN-OS 5.0, the failure of a software agent to properly determine the hardware model caused intermittent dataplane start issues.

- 46477—The DHCP client on the firewall was sending an invalid option (option 54) in its renewal requests, causing the DHCP server to ignore the requests.

- 46367—Performing an AV update directly after a Validate candidate configuration operation was causing the temporary candidate configuration files to be written to the running configuration. The next time the configuration was reloaded (commit, content update, or restart), the candidate configuration would then become the running configuration.

- 46296—Although the firewall allowed configuration of a RADIUS server profile that included a subnet mask at the end of the IP address, this configuration would cause authentication to fail. The firewall now strips the subnet mask from the server profile configuration before saving it.

- 46184—When using link monitoring to monitor SFP Plus ports on PA-5000 Series devices, there would sometimes be a delay in detecting the link failure after the system time was set backwards because the timestamp of a state change was not being checked on these ports.

- 46168—Sometimes when deleting a security policy or a series of policies from the web interface, the wrong policies were deleted due to a mismatch between the internal row index and the table as rendered in the interface.

- 46157—Very large web-browsing sessions (over 4GB) were causing the dataplane to restart.

- 46052—Users attempting to authenticate to a GlobalProtect gateway were not able to connect if the user name contained a hash character (#). This issue has been resolved and the hash character is now allowed in the user name.

- 45965—When running the `test nat-policy-match` command on PA-200 devices, the test results were not displayed in the output.

- 45943—Fixed a firewall restart issue that occurred when a URL database update was triggered at the same time that a top-URLs report was being run. The database update process will now be on hold until the report is finished generating.

- 45859—Certificates containing an ampersand character (&) in the subject name could not be imported onto the firewall because special characters were not supported in the certificate fields.

- 45826—The built-in Active Directory groups were not displaying in the **Device > User Identification > Group Mapping** section of the web interface even though you could display them using the CLI.

- 45815—Fixed an SSH connection failure problem that occurred on multi-VSYS configurations and shared gateway deployments with zone protection profiles enabled with SYN cookies.

- 45811—When configuring a GlobalProtect gateway on a VLAN interface configured as a DHCP client, the configuration would fail to commit due to an error parsing the interface name.

- 45795—When using a traffic generator to send multicast traffic through PA-5000 Series firewalls for testing hardware offload, some packets were being dropped. Issue due to a problem occurring when sessions exist on one dataplane and the remaining dataplanes are not refreshed, causing the multicast FIB to age out.

- 45785—When deleting redistribution profiles that were referenced in an OSPF area from a virtual router, an error occurred, but did not provide the correct information. The error should have stated that the profile was being referenced in the OSPF area, so the admin would know to remove it from the OSPF area first, before deleting. Issue occurred when OSPF references a redistribution profile that was named using alphanumeric characters, when it should only use an IP subnet or a valid redistribution profile name.

- 45784—Users connecting to a network with GlobalProtect, which was configured with AD authentication, were showing that their passwords were going to expire in x number of days, even though a Group Policy Object specified a maximum password age of 0 (which means passwords do not expire). Previous work around required Individual accounts to be set with the Password never expires option turned on. Issue due to a problem with AD Authentication profile not recognizing the maximum password age setting of 0.

- 45649—When using the Classified option in a DoS profile and then applying that profile to a DoS policy, threat logs were not generated when the Alarm rate was exceeded. Update made to properly handle the Classified option.

- 45458—Zone-protection profiles were not displayed in the CLI output. Now, the CLI output for the `show zone-protection zone <zone_name>` command accurately displays the zone protection profile attached to a specific target VSYS or all VSYS that use the same zone name.

- 45259—Firewalls configured with active/active high availability (HA) in virtual wire mode were experiencing connection issues on inbound traffic. Problem occurred when DoS protection was configured with the SYN cookie option enabled. Issue due to a race condition that occurred when processing client responses.

- 45187—Firewalls with multiple virtual systems enabled were showing shadow policy warnings for other virtual systems during a commit. This was occurring with device admins that only had access to a given VSYS and not the other VSYS instances that contained the conflicting configuration. Update made to only show commit issues related to the virtual systems that the admin has permissions to manage.

- 44805—When a user entered incorrect login credentials and was locked out of the firewall, you could not unlock the user account using the web interface when an authentication sequence or an authentication profile was defined for the user. This issue is now resolved; the web interface permits you to unlock the user account.

- 44776—Admin was not able to modify a zone name if the zone location was set to a shared gateway.

- 44250—The Panorama management server stopped responding when doing a filter query from the traffic logs page. Issue due to the corruption of a log index file that occurred when upgrading to a new PAN-OS feature release. Preventative measures put in place to prevent issues with the log conversion process that occurs when upgrading between feature releases.

- 44184—Custom vulnerability profile was not saved after upgrading the firewall to a newer release and had to be re-created. The issue was caused by a problem with the upgrade migration script related to vulnerability profiles.

- 43665—Admin was not able to unlock another admin account that was locked after failed log in attempts when an authentication sequence was configured to check the LDAP profile and then the local profile.

- 42960—VPN tunnel between Cisco ASA and Palo Alto Networks firewalls configured in an active/passive high availability (HA) configuration failed to recover the tunnel when failing over to the passive device after upgrading PAN-OS on the active device. Issue due to problems with synchronizing the IPSec sequence numbers between HA devices.

- 42439—When a VSYS is configured with a shared gateway, Microsoft Express updates were not working properly. Issue was due to a problem with the firewall not being able to process cross VR traffic on PA-2000 Series devices.

- 42322—PA-5000 Series devices in a high availability (HA) active/active configuration were experiencing failures with the packet processing engine, which caused failovers to occur. Issue due to problems with packets that were passed over the HA ports, which may have been caused by the intermediate device connecting the two the firewalls.

- 41439—The route daemon on the firewall in a high availability (HA) configuration was consuming a large amount of memory and causing system daemon problems when large numbers of routes were received from BGP peers. Improvements implemented to better handle route distribution between the management plan and dataplane to reduce memory consumption.

- 40520—Discrepancies seemed to be appearing when running two different reports that should produce identical outputs for a threat report and a threat summary report. In this case, the data being collected was correct, but due to the time intervals in which the report was being invoked, the reports seemed to be inconsistent. For example, when the report thread is invoked, it may not start exactly on the hour and may be offsite slightly and will be written every 15 minutes. If the report starts 5 minutes past the hour, it will run at 5 minutes past the hour, at 20 minutes, 35 minutes, and then again at 50 minutes after the hour. Also, if summary logs for the last 15 minutes are written into the current 15 minute interval, the log may be written to the next time slot. For example, summary logs from 10:45 AM to 11 AM may be written to the 11:00AM to 11:15 AM time slot and may show the same receive time as when the summary timer was triggered. An update has been made to generate the summary reports at the 0, 15, 30, and 45 minute boundary.

- 37540—Adding an IP address to a predefined region was overriding the predefined region geo location, which caused issues with policies and when trying to view traffic information from the **Monitor > App Scope > Traffic Map** feature. This occurred when adding a custom region using the same name as a default region. An update has been made to combine the custom and default region IP information in this scenario. A cosmetic issue was also addressed, which will cause the map to use the default predefined latitude and longitude if the custom region does not specify longitude and latitude.

Addressed Issues 5.0.1

- 46329—Active device in a high availability (HA) configuration went to non-function on PA-5000 Series firewalls due to a segmentation fault.

- 46285—Resolved the issue where QoS statistics were not displaying in the web interface.

- 46224—When pushing a Captive Portal rule from Panorama 5.0 to a PAN-OS 4.1.x firewall, the correct action was not pushed. Issue was due to a change made in 5.0 for the two actions: ntlm-auth and captive-portal. In 5.0, the rules are web-form and browser-challenge. Update has been made to correctly map the differences, so browser challenge maps to ntlm-auth and captive-portal maps to web-form.

- 46136—After enabling GlobalProtect on the firewall, agents connecting to the portal or gateway would sometimes receive an error code stating that a specific path could not be found on the firewall. The response page has been changed so that it now only shows an HTTP 404 Not Found error, rather than revealing the path.

- 46076—Nested address groups or address groups with multiple objects referenced in NAT policy rules were causing the device to restart due to a parsing error.

- 46059—Session timeout settings were not in effect when set to the maximum value.

- 46014—Policy rules with schedule settings that rolled over into a second day (for example, 13:00-01:00 instead of 13:00-23:59 00:00-01:00) were not being enforced.

- 46005—When using the on-device User-ID agent in a configuration where it uses a data port to communicate with the Active Directory domain servers to join the domain, the device was going into a loop and could not start up due to autocommit failures. The workaround for this issue was to use the MGT port to contact the AD servers, which is the default configuration.

- 45994—Actions in the web interface, such as saving an object or performing a commit, were causing the firewall to be unresponsive in cases where the locked users list was very large (over 18,000 entries).

- 45975—FTP log exports were failing due to invalid escape characters in the login username sent by the firewall.

- 45942—In high availability (HA) active/active configurations, active sessions would sometimes break during failover if the HA3 link failure notification was received before the HA1 link failure notification. To resolve this issue, the HA3 link down timeout has been increased.

- 45900—Resolved a template commit error that occurred after Panorama and a managed device were upgraded to 5.0. This error occurred on devices that did not have virtual systems enabled. With this fix, when pushing templates you can toggle between single- and multi-VSYS mode.

- 45899—User-ID mapping information was being dropped for Windows clients who stayed logged in for an extended period of time. This occurred intermittently when WMI probing was used.

- 45779—Fixed the syntax in the CLI to allow you to create a zone that specifies the interface type (L2, L3, v-wire) only, and without selecting the physical interface(s) that will be associated with the zone.

- 45775—The user was unable to log in to the Web and the SSH interface on the firewall because of a syntax error. With this fix, usernames in the NetBIOS (domain\user) and the UPN (user@domain.com) formats are interpreted correctly, and the user can successfully log in to the firewall.

- 45664—If an M-100 in log collector mode experiences a chassis failure and an RMA replacement for the chassis is received, you can move the RAID disk set from the failed chassis to the new chassis. If the Panorama server that is using the M-100 is in high availability (HA) mode, additional steps are needed to perform the disk move and to properly recover logs. For complete details on the steps needed to perform this operation when Panorama is in HA mode, refer to the tech note at https://live.paloaltonetworks.com/docs/DOC-4157.
  Note: These steps are not necessary if you are running Panorama 5.0.1 or later.

  This bug was not added until the 5.0.5 release. See the revision history table for more information.

- 45604—PA-200 device was experiencing latency issues and the device utilization was over 89% when an L2 sub-interface was configured on an L3 VLAN interface. Issue due to a packet buffer leak caused by an invalid port being set on the packets traversing the VLAN interface.

- 45566—The CLI command to identify the security rule that matches a specified user to the group the user belongs to did not work properly. The command, `test security-policy-match source-user <user> source <ip-address> destination <ip-address> destination-port <port no.> protocol <no.> from <zone> to <zone>` now accurately displays the user group information for the user.

- 45556—Administrator was not able to modify logging and reporting settings on the passive device in a high availability (HA) active/passive Panorama configuration. This part of the configuration was not synced, so when the active device was updated, the change was not synced to the passive device. Update made to allow disk quota for logging and reporting settings to be configured on a passive device.

- 45530—The first Encapsulated Security Payload (ESP) packet was being dropped after a high availability (HA) failover occurred causing issues with IP Phones on one side of the firewall attempting to communicate with a call server on the other side of the firewall. The first ESP packet was dropped, but remaining packets were received; the drop in the first packet caused the IP phones to reboot. Issue due to a hard-coded Security Parameter Index (SPI) that the firewall uses for pass-through IPSec.

- 45521—When configuring virtual wire sub-interface with VLAN "0" (untag), a VLAN other than 0 should be used in the tag allowed list of the main virtual wire (the virtual wire binding the physical ports); otherwise performance issues may occur.
  Leaving the tag-allowed empty doesn't trigger the VLAN comparison. The empty tag-allowed list is later tagged with VLAN "0", creating a situation where two interfaces will have the same key (port, vlan). This duplicate entry cannot be removed by updating the configuration. If this occurs, the dataplane must be restarted to fix this incorrect hardware entry.

- 45463—When a large number of groups (between 136 and the maximum of 640) were associated with security policies, the security policy would randomly lose groups and users associated with that security policy would fall through to the default policy. With this fix, the device accurately displays the groups that the user belongs to and applies the best match policy defined for the user group.

- 45294—NetFlow export was not working properly when more than one interface was set up for export.

- 45242—Fixed a display error in the inbound and outbound interfaces referenced in the threat logs.

- 45219—When an in-box failure occurs across one of two virtual wires being used for a network route, the SSL decrypt session information would not be persistent to the path that failed over. The decrypted session would fail and the user would have to re-establish their connection in order to access the requested content. This issue is now addressed, SSL decrypt information is being synced and the SSL session does not need to be requested again/reloaded, on failover.

- 45187—Firewalls with multiple virtual systems enabled were showing shadow policy warnings for other virtual systems during a commit. This was occurring with device admins that only had access to a given VSYS and not the other VSYS instances that contained the conflicting configuration. Update made to only show commit issues related to the virtual systems that the admin has permissions to manage.

- 44725—On PA-5000 Series firewalls, the decryption keys were not being properly synced to all dataplanes, which caused encrypted traffic on the other dataplanes to fail decryption.

- 44648—Panorama Scheduled Config Export was not working properly due to incorrect permissions being set on the config output. This caused access issues with the cron.d job, which is used to perform scheduled tasks.

- 44626—Received the error OSError: [Errno 28] in Panorama when trying to create a tech support file. Issue due to lack of space on the partition where the support files are stored (/dev/sda2) and was caused by a log rotation issue. A new cron job has been created for Panorama VM that will prevent this issue.

- 44452—The first TCP SYN packets were being dropped when TCP sessions traversed the firewall between two different virtual systems. The sessions were established after a second SYN was sent. Issue due to a race condition that occurred when the packets were sent between dataplanes.

- 44003—The virtual memory limit for Panorama was insufficient. This fix provides the Panorama superuser and admin-role with the commands `debug software no-virt-limit` and `debug software virt-limit` commands that previously only existed on PAN-OS firewalls. You can now adjust the virtual memory from 0-4294967295 (4GB) using the `virt-limit <value>` option.

- 43868—When running User-ID related CLI commands from the firewall for Active Directory user or group names that included special characters, the command produced an error. For example, `show user user-IDs match-user $usertest`. Update made to allow all characters, other than control characters.

- 43838—When URL filtering was enabled with an admin override for certain categories, when IE clients accessed a site that is in the defined category and invalid credentials are submitted three times, the site should be blocked and the client should not receive another login prompt. With this issue, no matter how many failed logins occurred, the user was continually prompted to log in and the site was not blocked. Update made to block the sites after three failed logins when using the enter key to submit credentials.

- 41113—User-ID group/user mapping information retrieved by the firewall using an LDAP profile was not able to be removed after removing the group mapping profile due to cache issues in the VSYS.

- 38822—Resolved the issue that caused a restart when the hardware offload chip entered a loop because of an error in the scan output.

Addressed Issues 5.0.0

- 45666—Packets were being dropped randomly when DHCP relay was enabled.

- 45623—The log password field was not being handled properly when administrators logged in to the firewall using client certificate authentication.

- 45563– On PA-200 devices, the “Chassis Master Alarm: Power” alarm was being triggered, even though no issues were occurring at the time. Issue due to the threshold being set too aggressively. Alert threshold has been changed from 11.4 volts to 11.1 volts in order to eliminate false alarms.

- 42250/45542/45821/43910—When creating an administrator account from the CLI, the SSH or Telnet session would terminate upon entry of the new administrator password.

- 45531—When removing a group in Active Directory, the User-ID group mapping on the firewall was being updated, but other groups were inadvertently being removed.

- 45518—This bug resolves the remaining issues that were found in bug 45340, where a 1% packet drop was still observed after the fix. Description for bug 45340: On PA-5000 Series devices, packet drops were occurring with IPv6 traffic due to issues broadcasting IPv6 packets to the dataplanes.

- 45349—PA-5050 device with multiple virtual systems configured restarted after configuring a new LDAP server for User-ID. The restart occurred when expanding the groups in the User Identification group-mapping page. Issue occurred because an LDAP server profile was not configured. Update made to not allow group expansion unless an LDAP server profile is created in **Device > Server Profiles > LDAP**.

- 45340—On PA-5000 Series devices, packet drops were occurring with IPv6 traffic due to issues broadcasting IPv6 packets to the dataplanes.

- 45205—User-ID agent on the domain controller configured with WMI probing with the default probing interval of 2 minutes and the Enable Security Log Monitor set to “no” could not retrieve user to IP mapping data for roaming users after changes were made to the agent, such as modifying the probing interval. Issue due to a stale flag that remained in the agent for the roaming user, so further attempts to probe for mapping information was not occurring.

- 45143/45186—Automatic configuration synchronization was not occurring between peers in a high availability (HA) configuration after a policy change. Status of the synchronization was not correct, the device that the configuration change was made on showed sync was complete, but the peer device showed it was in progress.

- 45000—Network latency was occurring on the firewall that was in FIPS mode with aggregate interfaces. The firewall was also configured to forward PE files to WildFire. Issue due to a problem with memory pool depletion with this configuration.

- 44935—Addressed a parsing error that displayed when committing data filtering rules in policy.

- 44889—Performing set commands on the firewall using the REST API was causing the Palo Alto Networks next-generation firewall management server to stop responding.

- 44792—Unexpected input in the management web interface was causing the management server to stop responding.

- 44760—Certificate Revocation List (CRL) checks were not able to reach the intended host to perform the certificate checks when a Blue Coat ProxySG was between the firewall and the host.

- 44758—Captive Portal authentication through a web proxy was failing due to an issue where Captive Portal was adding the proxy port (8080) to the URL after authentication. This caused an issue when trying to redirect the user to the intended website.

- 44586/45074—User-ID information was not getting updated for GlobalProtect clients running in environments that do not have gateway licenses.

- 44449—Resolved the issue that caused the inability to form an IPSec VPN tunnel, which led to a failure in processing traffic.

- 44444/45395/45771—A high availability (HA) active-primary device in an active/active configuration was having issues with dataplane restarts. Restarts occurred because of flapping on the firewall interface configured in virtual wire mode receiving asymmetric traffic from the neighbor router. Issue due to problems with HA session ownership handling.

- 44416—An IOS 6 device behind a NAT device failed to connect to GlobalProtect and displayed the error "Negotiation with the VPN server failed". This issue is now fixed and IOS 6 devices can successfully connect to Global Protect.

- 44408—Improved the time to commit and responsiveness in the web interface and the CLI on a firewall that constitutes a large number of multi virtual systems.

- 44330—Addressed a management plane restart issue that occurred on a configuration commit.

- 44247—The URL category information on an HTTPS request was not displayed in the response page that displayed when the "SSL Decryption Opt-out" option was enabled. This issue is now fixed; the URL category is included in the response page.

- 44113—Fixed a high availability (HA) failover issue that was caused by missed heartbeats, from the management plane, during initialization.

- 44067—Certain NetFlow analyzers unable to parse packets from the firewall due to a non-standard SNMP interface index.

- 44003—The virtual memory limit for Panorama was insufficient. This fix provides the Panorama superuser and admin-role with the commands `debug software no-virt-limit` and `debug software virt-limit` commands that previously only existed on PAN-OS firewalls. You can now adjust the virtual memory from 0-4294967295 (4GB) using the `virt-limit <value>` option.

- 43951—File blocking pages were displaying incorrect error messages when users attempted to upload blocked files.

- 43872—The block page for SSL traffic was not displayed when a policy match occurred for a URL filtering profile configured with a block action. With this fix, the SSL block page displays.

- 43726—In a high availability (HA) active/passive configuration with OSPF, when a failover occurred the adjacencies came up within a few seconds, but traffic did not start flowing again for approximately 18 seconds. Issue was due to the peer firewall waiting too long to before starting SPF calculations and in sending LSAs, which is now fixed.

- 43681—If you use Panorama pre and/or post rules to manage your devices and configure an address object that is invalid or doesn't exist on the device, the attempt to commit the rules would fail with an unclear message. Now, the error message on a commit failure indicates the problem with the address object.

- 43656—Botnet reports were inaccurate when the Browsing IP Domains option was disabled in the **Monitor > Botnet > Configure** tab. This issue is resolved and URLs for IP domains that are disabled are now excluded from the Botnet report.

- 43507/45468/45509/44991—SSL decryption was failing when attempting to view/download large files.

- 43399—For devices managed using Panorama, the GlobalProtect Portal license was displayed as “License Expired” in the **Panorama > Deployment > Licenses** tab. With this fix, the validity of the license is displayed accurately.

- 43323—In an active-active high availability (HA) configuration, a GlobalProtect Gateway configured with a floating IP address and configured for external authentication, failed to bind to the server; cannot assign requested address message was logged in the system logs of the on the active-secondary device.

- 43278—File blocking rules with the block and continue action were not working properly with .docx file types.

- 42968—Addressed an issue that caused a delay when downloading compressed zip files.

- 42561—Log export from Panorama was causing long response times and unresponsiveness from the web interface and CLI.

- 42575—–The hardware table on the firewall occasionally retained information on stale sessions. This issue is now fixed and the entries in the hardware table only match active sessions on the device.

- 42265 - Addressed a display error in the traffic log entry for sessions that were not decrypted, but were displayed as decrypted. This issue occurred when SSL inbound decryption (to decrypt traffic to a server) was configured and the certificate used in the policy was not the same as that on the server.

- 41966—If the GlobalProtect Portal or Gateway were configured in a zone with a zone protection profile configured for SYN cookies, then GlobalProtect clients were unable to connect to the Portal or Gateway over SSL. This issue is now resolved, and a GlobalProtect client can now make an SSL connection to a zone configured with SYN-cookie protection.

- 41929—Added performance improvements in Panorama to address the responsiveness issues when switching device context.

- 41927—Panorama VM and Panorama on the M-100 platform will periodically run a file system check (FSCK) in order to prevent corruption of the system files. During this time, Panorama will not be accessible until the check is complete. With this fix, when you attempt to log in to Panorama from the web interface or when using SSH, you will now see a message showing that the FSCK is in progress. The FSCK will run after 8 reboots or at a reboot that occurs 90 days after the last FSCK was performed.

- 41910—Added XML support for the `show system services` command. The API now displays the XML results for the request.

- 41670—Resolved the issue that caused a spike in interface utilization traffic on the monitored interfaces, when SNMP was enabled.

- 41347—Packet capture filters were not filtering information accurately. The fix ensures that the pcap filters match the criteria defined on the device and accurately capture all relevant frames in the session.

- 40643—When remote users authenticate to the firewall using an RSA server that is configured to use User Principal Name (UPN) style login (user@domain.com), the firewall did not authenticate the user due to an issue interpreting the UPN format.

- 40625 - When authenticating to an LDAP server that was not a Microsoft Active Directory server, authentication issues occurred because the modify timestamp option was included in the LDAP query to the LDAP server. To resolve this issue, a new configuration option use-modify-for-group-mapping has been added in the CLI. This setting allows the user to configure whether or not the timestamp is sent in the LDAP query to the server.

- 37008—The display output of the `show routing route destination address` command was showing incorrect data due an issue where only first byte of the IP address was being compared.

- 35989—When using a custom log format, the information displayed in the report was inaccurate for multiple traffic log entries for different source users. The issue has been fixed and the report accurately reflects the data on traffic per user/IP address.

- 28222—Attempts to export log files to a comma separated values (CSV) file were failing when the number of rows to export was set to the maximum value (1,048,576). This problem was occurring on some platforms because the large size of the export file required memory allocation beyond the device capacity. The way the logs are exported has been changed so that memory allocation is no longer an issue and the maximum number of rows will now export to CSV successfully on all platforms.

Known Issues

Note: Starting with PAN-OS 5.0.20, 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.

This following is a list of known issues in PAN-OS 5.0 releases:

- 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.

- 55111—A TCP session in PAN-OS does not tear down for 30 seconds after receiving a FIN packet. In some network environments, such as those using a proxy server, the client sends a SYN packet using the same source port within 30 seconds after sending a FIN packet, which causes the firewall to drop subsequent packets when it determines that the TCP sequence number is "out of sync."

  Workaround: Configure the firewall to bypass asymmetric paths using the `set deviceconfig setting tcp asymmetric-path bypass` Configuration mode command.

- 50817—When the external-facing interface on a GlobalProtect gateway is configured with dynamic PPPoE and a loopback interface is configured for the destination interface to the GlobalProtect portal, GlobalProtect users cannot connect. This issue occurs in PAN-OS 4.1.6 and later releases when the gateway is unable to determine the tunnel ID of the portal in this configuration.

  Workaround: Do not use a loopback interface; use only the PPPoE interface in this configuration.

- 49040—By default, the WildFire Server in the WildFire General Settings section (**Device > Setup > WildFire**) is set to `default-cloud`. If you delete this value and attempt to restore it by re-entering the value in the field, the firewall will no longer be able to access the WildFire Portal when you attempt to view a WildFire report. If you inadvertently delete the value in this field and still want to use the `default-cloud` server setting, leave the field blank and **Commit** the change, which will restore the WildFire server `default-cloud` setting.

- 48709—The web interface automatically adds 0.0.0.0 as a packet capture filter but packet capture filters are not correctly applied when 0.0.0.0/0 is configured as the source or destination IP address.

- Workaround: Ensure that you do not use 0.0.0.0/0 for either the **Source** or **Destination** when configuring a packet capture filter (**Monitor** > **Packet Capture** > **Configure Filtering** > **Add** > **Packet Capture Filter**).

- 48599—When a source or destination address object is added through the CLI, and then the web interface is used to reference the object in a security policy, the address object is inaccurate. The object details displayed in the web interface do not match what was defined in the CLI.

  Workaround: Use the web interface to create the address object and then add it to Security policy.

- 45464—On the Panorama virtual appliance, summary logs for traffic and threats are not written after issuing the `clear log` command.

  Workaround: Restart the management server to enable summary logs.

- 45424—When you switch context from Panorama and access the web interface of a managed device, you might not be able 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.

- 45391—There is a limitation when configuring a management IP address on an M-100 appliance configured as the secondary passive peer in a high availability (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.

- 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**).

- 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. Once 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.

- 39623—If you add a decryption policy that instructs the firewall to block SSL traffic that was not previously being blocked, the firewall will continue to pass the unencrypted traffic.

  Workaround: Use the `debug dataplane reset ssl-decrypt exclude-cache` command to clear the SSL decrypt exclude cache.

- 39543—SSH host keys used for SCP log export are stored in the known hosts file on the firewall. In a high availability (HA) configuration, the SCP log export configuration is synchronized with the peer device, but the known host file is not synchronized. This causes SCP log export to fail upon failover to the peer device.

  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.

- 38261—New certificate authority (CA) certificates generated on the firewall are missing the "OCSP Sign" Extended Key Usage flag, causing certificate validation to fail with certain clients.

- 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.

- 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.

- 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.

Documentation Errata

This section lists outstanding issues related to the PAN-OS documentation.

- In the 5.0 *Palo Alto Networks Administrator's Guide* in chapter 8, the number of supported IPSec tunnels shows 10, the correct number is 250. To find this information, search the guide for "maximum of 10 IPSec tunnels". The paragraph should have stated the following: "Each tunnel interface can have a maximum of 250 IPSec tunnels (also known as Proxy IDs or bidirectional security associations). This allows you to set up IPSec tunnels for individual networks that are all associated with the same tunnel interface on the firewall.
  Note: Some platforms support fewer than 250 IPSec tunnels in total, so a tunnel interface capacity will be similarly limited. For example, the PA-200 supports 25 IPSec tunnels, so you could configure a single IPSec tunnel with 25 proxy IDs or five IPSec tunnels with five proxy IDs. In other words, you can configure 250 proxy IDs per IPSec tunnel as long as you do not exceed the maximum supported IPSec tunnel limit for the given platform.

- In the *Palo Alto NetworksM-100 Hardware Reference Guide* there was no description of the drive LEDs. The English version of this guide has been updated to rev B to indicate that the top LED on the drive will blink green when there is drive activity and the bottom LED will illuminate red when a drive failure has occurred.

- In the 5.0 *Palo Alto Networks Administrator's Guide* in the Firewall Logs section table Log Types and Settings, the Configuration description says that configuration log entries could not trigger SNMP traps. This is not true; you can send SNMP traps for configuration log entries.

- In the 5.0 *Palo Alto Networks Administrator's Guide* in the URL Filtering Profile Settings table, the Action on License Expiration is not correct for Block. If you are using the BrightCloud database and you set this option to Block upon license expiration, all URLs will be blocked, not just the URL categories that are set to block. If you set to Allow, all URLs will be allowed.
  If you are using the PAN-DB database, URL filtering will continue to function and the URL categories that are currently in cache will be used to either block or allow based on your configuration.

- In the 5.0 *Palo Alto Networks Administrator's Guide* in the Custom Syslog Field Descriptions section, the Threat Field table listed WildFire as a main field that could be used in the custom log format. This is not correct; WildFire is a value of the Subtype field for the Threat logs, so it is not available as its own field in the custom log format for the syslog server profile.

- In the 5.0 *Palo Alto Networks Administrator's Guide* in the DNS Proxy table, the description for Static Entries is incorrect. It stated that the FQDN field is for the DNS server. The correct description follows:
    - **Static Entries** - Provide static FQDN to IP address mappings that will be delivered in response to DNS queries made by hosts. Click **Add** and specify the following information:
    - **Name**—Enter a name for the **Static Entry**.
    - **FQDN**—Enter the Fully Qualified Domain Name (FQDN) that will be mapped to the static IP addresses defined in the **Address** field.
    - **Address**—Click **Add** and enter the IP addresses that map to this domain.

  Repeat to add additional addresses. To delete an address, select the address and click **Delete**.

- The VM-Series section of the *Palo Alto Networks Administrator Guide Rev A* states that only one instance of the VM-Series firewall can be installed on a single ESX(i) server. In the RevB version of the guide, this information has been updated to state that you can have more than one instance on a single ESX(i) server.

- The CLI command `show session rematch` was added in the 5.0 release, but was not documented in the CLI Reference Guide. This command can be used to show the statistics of the most recent session rematch processes when session rematch is enabled (`set device config setting config rematch yes`). The rematch process rematches all existing sessions against the updated policy rulebase when a new configuration is committed. The purpose of this option is to make sure that if a policy is changed to remove access to a given application, all current sessions will be ended.

Related Documentation

The following additional documentation is provided on the support site:

- **Getting Started Guide**—This guide takes you through the initial configuration and basic set up of your Palo Alto Networks firewall.
- **Administrator's Guide**—Describes how to administer the Palo Alto Networks firewall using the device's web interface. The guide is intended for system administrators responsible for deploying, operating, and maintaining the firewall.
- **PAN-OS Command Line Interface Reference Guide**—Detailed reference explaining how to access and use the command line interface (CLI) on the firewall.
- **Hardware Reference Guides**—Detailed reference containing the specifics of the various hardware platforms, including specifications, LED behaviors, and installation procedures.
- **Online Help System**—Detailed context-sensitive help system integrated within the PAN-OS firewall web interface.
- **Open Source Software (OSS) Listings**—OSS licenses used with Palo Alto Networks products and software:
  - PAN-OS 5.0
  - Panorama 5.0

Requesting Support

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

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

Revision History

Date	Release	Comment
9/30/2016	PAN-OS 5.0.20	• Added 5.0.20 Addressed Issues section.
6/22/2016	PAN-OS 5.0.19	• Added 5.0.19 Addressed Issues section.
4/22/2016	PAN-OS 5.0.18	• Added 5.0.18 Addressed Issues section.
1/15/2016	PAN-OS 5.0.17	• Updated to include a more prominent note about expiring certificates that is resolved under bug 86938 in 5.0.17 addressed issues and updated support information.
1/4/2016	PAN-OS 5.0.17	• Added 5.0.17 Addressed Issues section; scrubbed Known Issues section; updated title, company name and title in footer, and copyright paragraph to be consistent with new formats; changed copyright end-year to 2016; added new Revision Date paragraph in two places (Title page and end of document).
3/30/2015	PAN-OS 5.0.16	• Added 5.0.16 Addressed Issues section, added links to existing doc references and to OSS license information, and cleaned up some terminology.
12/22/2014	PAN-OS 5.0.15	• Added an additional item to the section “Changes in Default Behavior”. The Domain field for an LDAP profile in the web interface requires a different format for the domain name entry in PAN-OS 5.0.1 and later releases than what was previously required in PAN-OS 4.1.X and PAN-OS 5.0.0 releases.
11/24/2014	PAN-OS 5.0.15	• Added an additional item to the section “Changes in Default Behavior”. The change from PAN-OS 4.1.X releases to PAN-OS 5.0.X releases is related to the Domain field in an LDAP Server Profile. Documentation for this change is added in PAN-OS 5.0.15; however, the change applies to all PAN-OS 5.0.X release versions.
9/18/2014	PAN-OS 5.0.14 (release note revision C)	• Bug 66632 was removed from the list of Addressed Issues 5.0.14. This bug is open.

8/26/2014	PAN-OS 5.0.14 (release note revision B)	• Bug 63971 was removed from the list of Addressed Issues 5.0.13. This bug was fixed in PAN-OS 5.0.14 and is correctly under Addressed Issues 5.0.14.
12/24/2013	PAN-OS 5.0.10 (release note revision B)	• Bug 58257 is addressed in PAN-OS 5.0.10. The release note revision A did not list bug 58257 as an addressed issues. The 5.0.10 release note revision B lists 58527 as an addressed issue.
8/20/2013	PAN-OS 5.0.7	• Update made to bug 50133 in the PAN-OS 5.0.6 addressed issues section. This bug also addressed an issue where the IP-address/subnet mask format caused an issue when configuring a GlobalProtect portal external gateway address.
7/16/2013	PAN-OS 5.0.6	• Added 50817 as a known issue.
5/16/2013	PAN-OS 5.0.5	• Bug 48497 is listed in the 5.0.4 and 5.0.5 addressed issues lists because there was a minor change in the 5.0.5 release. See the description in the 5.0.5 section for details. • Documentation errata added related to the number of supported IPSec tunnels. • Known issue added for bug 48599. • Bug 45664 was added to the 5.0.1 addressed issues section. The bug was not listed previously, because it was found internally. Due to customer feedback, the bug was added to provide more details on the issue. • Made an update to 46405. Please read this bug in the 5.0.2 section for the update information. The following are duplicates of this bug - 47280/46424/45635.
3/6/2013	PAN-OS 5.0.3	• New item related to URL filtering license expiration and configuration log files added to the Documentation Errata section. • Bug 45899 was reported in the addressed issues section of the 5.0.1 and 5.0.2 release notes. This issued involved both PAN-OS 5.0.1 and User-ID 5.0.1, so verification on both was not completed until after the 5.0.1 release note was generated, so it was still open in 5.0.2 at which time it was verified again and passed a second round of verification. Removed from the 5.0.2 list, since it was fixed in 5.0.1.

		• Bug 44250 was reported in the addressed issues section of the 5.0.1 and 5.0.2 release notes. The issue still had minor problems in 5.0.1, so in 5.0.2 it was completely fixed, so the bug was removed from the 5.0.1 list.
1/14/2013	PAN-OS 5.0.2	• New item added to the New Features management section with the title "Translated Help". • Rev B. of the Palo Alto Networks Administrator's Guide has been posted. The update contains minor changes made since the release of PAN-OS 5.0. • See bug 47195 and a new Change to Default Behavior item related to the App-ID cache. In 5.0.2, the App-ID cache is no longer enabled by default. • Document errata item added related to the CLI command `show session rematch`.

Revision Date: November 17, 2016