PAN-OS Release Notes

Version 5.0.4

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 this release and the Documentation Errata section for issues found in the documentation. Also review the Known Issues and the Upgrade/Downgrade Procedures sections thoroughly prior to installation.

Contents

New Features

This section provides details of the features introduced in the PAN-OS 5.0.0 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 allow an application in security policy without explicitly allowing its underlying protocol. This support is available if the application can be identified within a pre-determined point in the session, and has a dependency on any of the following applications: HTTP, SSL, MSRPC, RPC, t.120, RTSP, RTMP, and NETBIOS-SS. Custom applications based on HTTP, SSL, MS-RPC, or RTSP can also be allowed in security policy without explicitly allowing the underlying protocol. For example, if you want to allow Java software updates, which use HTTP (web-browsing), you no longer have to allow web-browsing. This feature will reduce the overall number of rules needed to manage policies.

- **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. The firewall can now be configured 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-User mapping for the User-ID Agent, Captive Portal, User-ID XML API, and Terminal Server agent, as well as IPv6 as the protocol 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** – In the User Activity Report a new column has been added to some sections to show 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 get the new brows time data going 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 firewall's 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 certs.
    - Block SSL sessions with untrusted server certs.
    - 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 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 hit 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.

- **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, 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. By doing this, a company can 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. Examples of 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. One specific example of how the pre-logon feature works is if a remote user forgets his/her password, since GlobalProtect would connect and use the cached credentials and establish a VPN before the login prompt even appears, a domain administrator could reset the user's password as if they were 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, which includes 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 to a given languages, the help content for that language will appear when clicking any of the Help icons.

- **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** – 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-based REST API Enhancement Import/Export** – The REST 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 admins, device admins, and role-based admins. Panorama admins can also run device-targeted API queries.

- **XML-based REST 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 may 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 encryption. 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 list shows services that are supported using IPv6:
    - Service Route 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 that TFTP is not supported because IPv6 support is not prevalent.

- **Certificate Management –** Enhancements have been made to improve the workflow and management of certificates. The **Device > Certificates** section has been 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 on by default and 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:

- 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.

Upgrade/Downgrade Procedures

The following sections provide upgrade/downgrade procedures and detail how certain features are migrated.

Upgrading PAN-OS

Important	In order to upgrade to PAN-OS 5.0.0, the device must be running PAN-OS 4.1 or later. Attempts to upgrade to PAN-OS 5.0.0 from earlier releases will be blocked.

Step 1: Get Content Updates

The device must be running content update 320 or later to upgrade to PAN-OS 5.0.0. Use the following steps to perform a dynamic content update, which consists of App-ID updates as well as threat updates depending on your subscription licenses. The device must be registered for the following steps to work. Please go to https://support.paloaltonetworks.com to register your device.

1. Navigate to the Device tab in the web interface and click the Dynamic Updates link.
2. Click Refresh to retrieve the currently available updates that can be installed.
3. Download the latest update to the device by clicking the Download link in the row corresponding to the latest update.
4. Once downloaded, click the Install link to perform the update.

Step 2: Upgrade the Software

Use the following steps to perform a software upgrade to this release:

1. Ensure the device is connected to a reliable power source as a loss of power during the upgrade could make the device unusable.
2. Navigate to the **Device** tab in the web interface and click the **Software** link.
3. Click **Refresh** to retrieve the currently available releases that can be installed.
4. Locate the latest release and download it to the device by clicking the **Download** link in the row corresponding to that latest release.
5. Once downloaded, click the **Install** link to perform the upgrade.

Downgrading PAN-OS

Important: In a major release (where the first or second digit in the PAN-OS version changes, example PAN-OS 4.0 to 4.1), the configuration may be migrated to accommodate new features, so you should not downgrade unless you also restore the configuration for that release. Maintenance releases can be downgraded without having to worry about restoring the configuration. Unmatched software and configurations can result in failed downgrades or even force the system into maintenance mode. If you have a problem with a downgrade, you may need to enter maintenance mode and reset the

device to its factory default configuration and then restore the configuration from the original config file that was exported prior to the upgrade.

1. Save a backup of the current configuration file by navigating to the **Device > Setup > Operations** tab, selecting **Export named configuration snapshot** > **running-config.xml** and clicking **OK** to save the configuration file. This backup can be used to restore the configuration if you have problems with the downgrade and you need to do a factory reset.
2. Navigate to **Device > Software** and you will see the software page that lists all PAN-OS versions that can be downloaded, or that have already been downloaded.
3. To downgrade to an older maintenance release, click **Install** in the **Action** column for the desired release. If the version you want to use shows Download, click the **Download** link to retrieve the software package and then click **Install**.

   Note: If you are downgrading to an earlier major release, navigate to the page that shows that release. When you click the **Install** link, you will see a pop-up that shows an auto-save configuration (as of 4.1). This configuration is automatically created and saved when you upgrade to a major release and should be used when downgrading to restore PAN-OS to the configuration that was present before the upgrade to the major release. For example, if you upgrade from 4.0 to 4.1, the auto-save configuration is created and can be used to downgrade back to 4.0. If you upgrade from PAN-OS 3.1 to 4.0, the auto-save configuration is not saved, so you will need to do a factory reset and restore your configuration manually.

4. After PAN-OS has been downgraded, click **OK** to reboot the device to 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 sections list the addressed issues for this release.

Addressed Issues 5.0.4

The following issues have been addressed in the 5.0.4 release:

- 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—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. Issue due to a problem where the category list was not properly updated after a PAN-OS upgrade. Update 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 VSYS. 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 would occur 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 would not update if the WildFire signature was less than 12 hours old. An update has been made in this release 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 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. This issue has been resolved with this release.

- 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. This issue has been resolved with this release.

- 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 user 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. This issue has been resolved with this release.

- 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. This issue has been resolved with this release.

- 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. This issue has been resolved with this release.

- 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. This issue has been resolved with this release.

- 46364—The firewall experiences Radius authentication failures when running in FIPS/CC mode. This issue has been resolved with this release.

- 45687—When 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. This issue has been resolved with this release.

- 44844—Intermittent failures occurred when connecting a firewall using LDAP over SSL (LDAPS) to a server. This issue has been resolved with this release.

- 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". This Issue has been resolved with this release.

- 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

The following issues have been addressed in the 5.0.3 release:

- 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. This issue has been resolved.

- 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 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 can not 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 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.

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

- 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 an 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 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 an 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. This issue has been resolved.

- 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. This issue has been fixed.

- 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. This issue has been resolved.

- 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, 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 the total byte count. The issue has been resolved to count both client-to-server traffic 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 that was issued previously by a different DHCP server. Issue due to a problem where the firewall's 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

The following issues have been addressed in the 5.0.2 release:

- 47280, 46424, 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. In order for this fix to work properly, the User-ID agent must be at 5.0.1 or later.

- 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 config 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 firewall's 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 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 an HA failover was triggered.

- 46538 – In an 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. This issue has been resolved.

- 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 subnetmask at the end of the IP address, this configuration would cause authentication to fail. The firewall now strips the subnetmask 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 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 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 an 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 an 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

The following issues have been addressed in the 5.0.1 release:

- 46329 – Active device in an 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 active/active HA deployments, 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.

- 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 an 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 an 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

The following issues have been addressed in the 5.0.0 release:

- 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. This issue has been resolved.

- 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 an 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 firewall's 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 – 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 an 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 an 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 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. This issue has been resolved.

- 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.

Known Issues

This following is a list of known unresolved issues in this release:

For recent updates to known issues for a given PAN-OS release, refer to https://live.paloaltonetworks.com/docs/DOC-1982

- 49040 – By default, the WildFire Server field (**Device > Setup > WildFire > General Settings**) is set to the value defalt-cloud. If you delete this value and then attempt to restore it by re-typing this 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 inadvertenly delete the value in this field (but still want to use the default-cloud), leave the field blank and then Commit the change. This will restore the value to its default setting.

- 45871 – Some special characters in an SSL certificate subject prevent the certificate from being imported.

- 45810 – A TCP session in PAN-OS will wait for 30 seconds to tear down after receiving a FIN packet. In some network environments, such as environments where a proxy server is deployed, the client will send SYN using the same source port within 30 seconds after it sends the FIN, and this will cause the firewall to drop subsequent packets because it detects the TCP sequence number as "out of sync." To work around this issue, configure the firewall to bypass asymmetric paths using the `set deviceconfig setting tcp asymmetric-path bypass` command.

- 45464 – Summary logs for traffic and threats are not written after issuing the `clear log` command. You must restart the management server to enable summary logs.

- 45424 – When performing a context switch from Panorama to a managed device, the PAN-OS software image upload may not work. If this issue occurs, use the **Panorama > Device** Deployment feature instead.

- 45391 – Limitation in configuring a management IP address on an M-100 configured as the secondary passive device in an HA pair. Workaround: To set the IP address for the management interface, you must suspend the active Panorama peer, promote the passive peer to active, change the configuration, and reset the active peer to the 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. To resolve this issue, enable the firewall to include the IP address of the firewall as the hostname in the syslog header by selecting the **Send Hostname in Syslog** check box on the **Device > Setup** page.

- 44571 – If a Panorama log collector MGT port is configured with an IPv4 address and you only want to have an IPv6 configured, you can use the Panorama web interface to configure the new IPv6 address, but you cannot use Panorama to remove the IPv4 address, you must use the CLI.

  To do this, you first configure the MGT port with the new IPv6 address and then apply your configuration to the log collector and test connectivity using the IPv6 address to ensure that you do not lose access when the IPv4 address is removed. Once the log collector is accessible using the IPv6 address, go to the CLI on the log collector and remove the IPv4 address and then commit. For example, to delete the IPv4 address on the MGT interface on a log collector, run `delete deviceconfig system ip-address.`

- 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 undecrypted traffic until the SSL decrypt exclude cache is cleared using the `debug dataplane reset ssl-decrypt exclude-cache` command.

- 39543 – SSH host keys used for SCP log export are stored in the known hosts file on the firewall. In an HA configuration, the SCP log export configuration is synchronized with the peer device, but the known host file is not. This causes SCP log export to fail upon failover to the peer device. To work around this issue, make the peer device active and then confirm the host key to ensure that SCP log forwarding will continue to work after failover.

- 38261 – New CA certificates generated on the firewall are missing the "OCSP Sign" Extended Key Usage flag, causing the 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 click the **Test SCP server connection** button after the template is pushed. The connection is not established until the firewall accepts the host key for the SCP server.

- 35352 – QoS profile selection based on source subinterface is not supported on PA-5000 Series or PA-3000 Series devices.

- 33612 – Attempts to reset the Master Key from Panorama (web interface or CLI) 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 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**.

- Known Issue bug 45521 was fixed in 5.0.1, but was not moved to the 5.0.1 Addressed Issues list until this release 5.0.3. It also did not state the bug number in the description.

- 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.

- The bug description for bug 44003, which was fixed in PAN-OS 5.0.0 has been updated in the 5.0.1 release note.

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 with the firewall's web interface.

Requesting Support

For technical support, call 1-866-898-9087 or send email to support@paloaltonetworks.com.

Revision History

Date	Release	Comment
3/6/2013	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	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`.