PAN-OS Release Notes

Version 5.0.1

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. These options can be enabled from the Network Tab then Network Profiles > Zone Protection > Packet Based Attack Protection and the IP Option Drop section.

- **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 remote users forget their passwords, a helpdesk admin can reset their domain passwords and the users can log in with the new password because the VPN is already established and direct domain authentication will work.

MANAGEMENT FEATURES

- **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://support.paloaltonetworks.com Technical Documentation.

- **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 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 workflow for adding threat exceptions from the Monitor > Logs > Threat details has changed. In prior releases, when you click 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 and click Export named configuration snapshot, select running-config.xml and click 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 section contains addressed issues for this release.

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.

- 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.

- 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.

- 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.

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

- 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

- 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.

- 45639 – When using the firewall to generate a Certificate Signing Request (CSR), which is located in **Device > Certificate Management > Certificates**, you can generate the CSR and use the **Signed by** drop-down **External Authority (CSR)**, but once the CSR is signed by the external authority, the import process will not function properly. You will need to submit a CSR using traditional methods until this issue is resolved.

- 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.

- 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 configuration log export (**Panorama > Scheduled Config 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.

- 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:

- **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.