PAN-OS Release Notes

Version 4.1.0

This release note supplements the PAN-OS 4.1.0 release. Refer to the Addressed Issues section for details on what has been fixed in this release. Please review the Known Issues and the Upgrade/Downgrade Procedures sections thoroughly prior to installation.

Contents

PAN-OS 4.1 New Features

APPLICATION IDENTIFICATION FEATURES

- **H.323 ALG Enhancements –** The H.323 VoIP application-level gateway (ALG) has been enhanced to support dynamic prediction of media sessions (pinhole opening) based on the signaling data, as well as payload modification when performing address translation on the traffic allowing NAT/PAT traversal for H.323 VoIP traffic.

- **URL Category in Match Criteria –** URL Categories can now be used as a matching criterion in the Security, QoS, and Captive Portal policies. This feature will simplify security policy creation when enforcing specific web-filtering policies by users and domain groups. QoS policies can be created to rate-limit traffic associated with specific URL categories. Captive Portal policies can be created to conditionally authenticate users based on the URL category of the website a user visits.

USER IDENTIFICATION FEATURES

- **User-ID Agent Consolidation –** The User-ID functionalities of User-ID Agent for Active Directory and User-ID Agent for LDAP have been consolidated into the new unified User-ID Agent that incorporates support for Active Directory, eDirectory, and the XML-API.

- **Active Directory Support Enhancements –** Several enhancements have been made to the User-ID capability relative to Active Directory environments:
  - Multi-domain/Forest support
  - Domain Controller auto discovery
  - PAN-OS-based group mapping configuration

- **Exchange Server Event Log Monitoring –** The new User-ID Agent can be configured to monitor logon events on Microsoft Exchange Server associated with Microsoft Exchange compatible client applications. This will allow the mapping of users that potentially do not authenticate to a Domain Controller but are authenticating to Exchange.

- **NTLM Authentication Enhancements –** Captive Portal NTLM authentication can now be configured to leverage multiple User-ID Agents to verify NTLM responses received from client browsers. In addition, if NTLM authentication fails, the user is now redirected to an explicit logon page instead of being presented with an error message.

- **Agent Status in Web Interface –** A new Connected column has been added to the User-ID Agent and Terminal Server Agent tables to show the status of the connection to the agents.

CONTENT INSPECTION FEATURES

- **Rule-based Vulnerability Protection Profiles –** The anti-spyware and vulnerability protection profiles have been enhanced to allow granular rule creation for adding signatures to the profile. These rules will apply to all existing and new signatures when they are added via content updates. Instead of selecting between simple and custom profiles, rules will be used in conjunction with an exception list which can change any individual signature behavior/action.

- **WildFire –** The file blocking profile action list has been enhanced to include a "forward" action, which will copy and forward files matching the policy to the WildFire cloud-based malware detection service. WildFire currently supports Windows PE files (executable files), and will run submitted files in a cloud-based sandbox environment to analyze the sample for malicious behavior. An administrator can view reports of submitted samples through the WildFire web portal at wildfire.paloaltonetworks.com, and can configure automated email reports.

NETWORKING FEATURES

- **Multicast Routing –** Allows the firewall to route multicast streams using PIM Sparse Mode (PIM-SM) and PIM Source-Specific Multicast (PIM-SSM). The firewall can also act as an IGMP querier for hosts that are on the same network as the interface on which IGMP is configured. PIM and IGMP may be enabled on layer 3 interfaces. IGMP v1, v2, and v3 are supported.

- **DHCP Client –** Allows a layer 3 interface to act as a DHCP client and receive a dynamically assigned IP address.

- **DNS Setting Propagation –** Allows the firewall to propagate DNS server and other settings from a DHCP client or PPPoE client interface into a DHCP server configuration. These settings may also be propagated to GlobalProtect gateway configurations.

- **NAT within Virtual Wire –** Allows the firewall to perform network address translation when deployed in virtual wire mode.

- **SHA-2 VPN Support –** Extends the list of supported authentication algorithms to include SHA-2.

GLOBALPROTECT FEATURES

- **Unification of NetConnect and GlobalProtect –** The feature set of NetConnect has been integrated into GlobalProtect. GlobalProtect in its base functionality now replaces NetConnect. The advanced functionalities of GlobalProtect, such as Host Information Profiles as well as multi-gateway support remain licensed features while single gateway configurations with no HIP capability will be available without a license.

- **Mac OS X Support –** GlobalProtect is now available for Mac OS 10.6 and 10.7 on 32 and 64 bit platforms.

- **Apple iOS Support –** Apple iOS devices can now establish IPSec connections using the native iOS IPSec client to a GlobalProtect gateway.

- **Client Override Enhancements –** A challenge-response based feature has been been added to allow for more flexible and controlled user overrides in GlobalProtect. Additionally, an administrator can specify the maximum number overrides a user can perform before a connection to a gateway is required.

- **User/Group-based Portal Configurations –** The GlobalProtect Portal now supports multiple agent configurations on a per-user or user-group basis within one portal configuration.

- **Gateway Selection Priority –** The mechanism in which GlobalProtect Agent selects the best available gateway has been improved with a priority rating for each external gateway. The gateway priority, from 1-5 in which 1 is the highest priority, allows administrators to influence which gateway will be chosen under normal operations.

- **Response Page Enhancements –** New response pages have been added to GlobalProtect to allow administrators to define a custom welcome and help pages as well as rich pages in response to specific HIP object matches.

- **Agent UI Control –** A new option has been added that allows administrators to change the visible UI options of GlobalProtect agent.

NETCONNECT SSL-VPN FEATURES

NetConnect functionality has been merged with GlobalProtect. With PAN-OS 4.1, the NetConnect agent and portal components are migrated to GlobalProtect. To cover the NetConnect functionality, basic GlobalProtect functionality is now available to all customers with no license. A GlobalProtect Portal license is still required for multi-gateway deployments and a GlobalProtect Gateway subscription is required for host profiling capability. Refer to the GlobalProtect section for all new features related to NetConnect functionality.

MANAGEMENT FEATURES

- **Report Translation –** Capability to customize the language used in report headers. The supported languages are Chinese (Traditional and Simplified) and Japanese.

- **Granular Commit Operations –** When performing a Commit operation, an admin now has the ability to specify which area of the configuration to commit. This allows an admin to commit policy related changes without committing in-process networking and device configuration changes. Additionally, in Panorama, the admin is now given a choice of whether to combine the Panorama configurations with the current running configuration on the device or with the candidate configuration on the device.

- **Detailed Configuration Logging –** The configuration logs have been extended to include before and after fields to display the details of every configuration change. These details can also be included when forwarding logs to external systems.

- **Customizable Logos –** The various company logos in the web interface and reports can be customized.

- **Log Database Enhancements –** Several performance and scalability improvements have been made to the log database including data compression, seamless format migration, indexing optimizations, and data summarization for query optimization.

- **Web Interface Update**s **–** The interface update that began in PAN-OS 4.0 is now complete. All areas of the web interface now leverage the same dynamic framework. In addition, performance optimizations have been done to improve tab switching and content loading performance.

- **Netflow –** The system can generate and export Netflow Version 9 records with unidirectional IP traffic flow information to an outside collector. Netflow exporting can be enabled on any ingress interface in the system. Separate template records are defined for IPv4, IPv4 with NAT, and IPv6 traffic, and PAN-OS specific fields for App-ID and User-ID can be optionally exported. This feature is available on all platforms except the PA-4000 series.

- **Structured SNMP Trap MIB –** A new MIB module has been added to define all SNMP traps generated by the system. Each system log in the system is now defined as an independent SNMP trap with an Object ID (OID) of its own, and individual fields in a log are defined as a variable binding (varbind) list.

- **XML-based REST API Enhancements –** The REST API for both PAN-OS and Panorama has been expanded to support all operational commands, several new configuration commands, commit operations, and packet-capture (PCAP) exports. Examples of supported operational commands include setting, showing, or clearing runtime parameters, saving and loading configurations to disk, retrieving interface or system information, etc. The newly supported configuration commands include get, rename, clone, and move.

- **SSH Key-based Authentication –** Key-based authentication of administrators for CLI access via SSH has been added. This will enable easy programmatic access to the device via automated scripts, without requiring a password to be entered. Each admin account contains an option to turn on public key authentication for SSH and to import a public key.

Changes to Default Behavior

The following are changes to the default behavior made in 4.1.0:

- User-ID Agent client probing now uses WMI as the default instead of NetBIOS.
- Panorama Administrator Access Control – When managing administrator accounts in Panorama, granting role based access to a Device Group no longer implies permissions to each device and virtual system on a context switch. You can now set granular access to each device under Panorama management by going to the Administrators account and selecting the device and virtual system under the Device Context tab. When the administrator logs in, they will only be able to do a Context switch to the device and virtual system to which they have access. This same functionality also applies to Access Domain in which an external authentication server such as Radius can be used to control access.

  Current administrator accounts that have a defined list of device groups will be migrated to have the same permissions when switching context. You will now see those devices and virtual systems selected in the Device Context tab, which will allow you to apply more granular permissions if needed.

Upgrade/Downgrade Procedures

The following lists information related to the upgrade/downgrade procedures of the firewall as well as details related to how certain features are migrated.

Important	In order to upgrade to PAN-OS 4.1, the device must be running PAN-OS 4.0.0 or later. Attempts to upgrade to PAN-OS 4.1 from earlier releases will be blocked.

- 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. Save a config backup by clicking Save named config snapshot. This can be used to restore the configuration in the event of a migration failure.

3. Navigate to the Device tab in the web interface and click the Software link.

4. Click Refresh to retrieve the currently available releases that can be installed.

5. Locate the latest release and download it to the device by clicking the Download link in the row corresponding to that latest release.

6. Once downloaded, click the Install link to perform the upgrade.

The device must be running content update 257 or later in order to upgrade to PAN-OS 4.1. Use the following steps to perform a dynamic content update, which consists of App-ID updates as well as threat updates depending on 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.

In the event the device needs to be downgraded the following procedure should be followed:

1. Enter maintenance mode and reset device to factory defaults.

2. Upgrade content and URL database to latest versions.

3. Restore configuration from original config file that was exported prior to upgrade.

- **Rule-based Vulnerability Protection Profiles Backward Compatibility**
  When upgrading Panorama or PAN-OS to 4.1, simple style vulnerability protection and anti-spyware profiles are automatically converted to rules of equivalent meaning. Custom style profiles are converted to exceptions that specify signature-specific actions, with no rules required.

- **NetConnect to GlobalProtect Migration**
  When upgrading to PAN-OS 4.1 on a firewall that is configured with NetConnect, the feature set of NetConnect will be integrated into GlobalProtect. It is important that you carefully plan your rollout of the GlobalProtect client to existing NetConnect clients to ensure uninterrupted service for your remote users.

  You should be aware of the following changes after the upgrade:

  - When upgrading your firewall to 4.1, NetConnect will be replaced by GlobalProtect and the NetConnect configuration will automatically migrate to a single portal/single gateway GlobalProtect configuration.
  - In the WebUI, the **NetConnect** side menu in the **Network** tab will be replaced with **GlobalProtect**.
  - GlobalProtect users will automatically be upgraded to the new GlobalProtect client when they connect to the upgraded portal.
  - NetConnect clients that connect to the upgraded firewall will be upgraded to the GlobalProtect client and the NetConnect client will be removed.

    Note: In order for a NetConnect client to upgrade to GlobalProtect, users will need administrative privileges on their system.

    You can choose to upgrade the client agent transparently, or you can prompt the user. If the **Agent Configuration** is set to prompt, the user will be prompted to select a 32-bit or 64-bit version of the client. After the GlobalProtect client installs, a VPN connection will be established using the new GlobalProtect client. To control the client install method, go to the WebUI on your firewall, select the **Network** tab > **GlobalProtect**, then click your portal name. In the **Agent** tab, you will see options for the **Agent UI** and under **Agent Configuration** you will see **Client Upgrade** with options for **prompt** or **transparent**.

  - Basic GlobalProtect functionality does not require a license. For additional functionality, the portal license is required for multi-gateway deployment and the gateway subscription license is required for host profiling.

  For more information, refer to the GlobalProtect Features section in this release note and the Palo Alto Networks Administrator's Guide.

- **User-ID Agent Upgrade**
  After installing PAN-OS 4.1, you will need perform the following steps before upgrading to the new User-ID Agent:

  Note: The new 4.1.0 User-ID Agent replaces the old Pan Agent service and User-ID Agent.

1. Add your directory server information in the Device tab > Server Profiles > LDAP configuration.
2. In the Device tab > User Identification > Group Mappings Settings tab, add the LDAP server that you configured in the previous step.
3. Upgrade to the new User-ID Agent.

Associated Software Versions

Software	Minimum Supported Version with PAN-OS 4.1
Panorama	4.1.0
User-ID Agent (AD)	3.1.0
User-ID Agent (LDAP)	3.1.0
Terminal Server Agent	3.0.0
NetConnect	1.1.0
GlobalProtect Client	1.0.0

Addressed Issues

The following issues have been addressed in this release:

- 33173 – QoS show output is not the same on the PA-2000 Series and PA-5000 series devices. The WebUI is "one" based on both devices, but in the CLI on the PA-5000, it's "zero" based.

- 32995 – Management plane stopped responding on the passive device in an HA pair. Issue related to ARP flooding, possibly due to a loop in the adjacent network configuration. Modifications made to better handle ARP flooding.

- 32759 – Error occurred in Panorama when trying to unlock a device admin account authenticated through LDAP or Radius. Issue was related to not correctly reading the / between the domain and user name.

- 32680 – Some pages within the device management WebUI may be vulnerable to cross-site scripting, which could lead to Cross-site Request Forgery (CSRF) attacks.

- 32658 – When trying to use inbound URL filtering to control access to a Webmail server for employees, certain client browsers were allowed access to the root of the Webmail server.

- 32583 – Root partition low on disk space caused issues with HA. Multiple User-ID logs were being exported as well as tech support files caused the partition to fill up. Modifications have been made to write such log files into a single file and to clear temporary files when a login session is not gracefully closed.

- 32564 – In an HA pair, the traffic log "from" zone was not matching the session or security policy.

- 32561 – In an HA active/passive configuration, the active node was non-functional after disabling state synchronization. Issue occurred because the higher priority device took over. Update made to prevent failover in this condition.

- 32522 – In custom reports the "Sessions" column name is appearing in CSV format, but in the PDF report the column name is "Repeat Count". PDF report has been updated to show "Sessions" for this column name.

- 32520 – With some custom reports, a "0" was omitted after the decimal point in the PDF output, the .csv file was fine. Issue related to formatting in the PDF export.

- 32289 – On a device with multiple virtual systems, when viewing bandwidth statistics in QoS view, only one VSYS showed details for applications, rules, and user ID. Update made so in a multi-VSYS device, all virtual systems will be displayed when viewing statistics.

- 32235 – When viewing logs from the WebUI, the management plane occasionally restarted. Issue related to the clock on the device rolling back to an old date and log index issues occurred.

- 32233 – URL filtering problems with web servers using IPv6 over HTTP proxy. URL parsing process has been updated.

- 32191 – Problems showing data in the admin timestamp column when running a config audit using Safari and Chrome browsers for the Mac.

- 32144 – While generating a tech support file in an HA pair, BGP peering started to have problems. Reports were also being generated at this time causing high CPU. Change has been made to pause batch processing while tech support files are generated.

- 31768 – Commit taking a very long time when the configuration had the maximum policies and objects configured on the device. More memory has been allocated in order to properly check options for the statistics upload service.

- 31764 – When trying to add or modify an admin role on a managed device from Panorama, when you click to update the account, your session is ended because Panorama is not using a Superuser account. Permissions have been added so Panorama can add and modify admin roles on managed devices.

- 31685 – SSL decryption was failing when a self-signed certificate was used. OCSP and CRL requests were timing out due to an issue with the protocol being used to push the certificate status from the management plane to the dataplane.

- 31683 – Issue controlling Facebook sub-applications, such as chat. The application decoder has been updated to thoroughly control all Facebook sub-applications.

- 31642 – While generating a tech support file in an HA pair, the management plane experienced high CPU and soon after HA heartbeats were missed, causing a fail over. Updates made to enhance the heartbeat mechanism.

- 31583 – HA problems after a power outage on adjacent switches with devices in active/passive HA mode with link monitoring enabled. Rapid state changes in HA occurred when the switches were restored and the Forwarding Information Base (FIBs) aged out the routing tables.

- 31582 – When creating a destination NAT rule with all valid settings, saving, then going back and changing the Source Translation to "none", the error "Failed to parse nat policy" is displayed. Issue only occurred when modifying the source translation in the "Source Translation" column. If you click to modify the entire NAT rule, it works fine. Source-translation type was missing when doing a commit.

- 31574 – When changing a custom URL filter profile action to "none" and clicking ok, the change reverts back to the last setting. Display issue was causing problems.

- 31573 – After installing new VSYS license and then adding more VSYS instances to a device via Panorama, the commit failed with the error "vsys id too big" because the new license was not recognized on commit. Update added to prevent commit error after additional VSYS licenses are installed.

- 31532 – When generating tech support file from Panorama context, the file size was only 1 byte, so the file had to be retrieved using SCP or TFTP.

- 31469 – The "show network interface ethernet" command is not showing details on a traffic interface configured as an HA port. The show command for HA interfaces has been updated.

- 31464 – When a role based admin in Panorama that has all permissions to Panorama, but not to the managed devices performs staged configuration changes for shared policies, proper locks were not occurring in Panorama and the admin could not commit, since they did not have permissions to the managed devices. This was an issue because some admins were responsible for prepping config changes and did not have commit permissions and other admins were responsible for checking and then committing the configurations. Logic has been put in place to properly handle config locks and commits in Panorama for the admins that only has Panorama access.

- 31358 – Schedule daily reports sent from Panorama not being emailed, but worked when generated manually from the managed device. Issues related to a problem in the PDF footer in the report.

- 30925 – Panorama not sending some reports and reports that are being sent do not have data. Problem only occurred with custom roles.

- 30865 – Problem accessing an Oracle database behind the firewall that uses a NAT'd address. Support added for Oracle NAT software support.

- 30824 – When multiple OpenLDAP servers exist in an LDAP server profile on the firewall, authentication starts to fail after a while. Fix has been applied to better handle OpenLDAP servers.

- 30685 – Domain user login names containing more than 31 characters are being locked due to an authentication failure when accessing a network through the firewall using SSL VPN or Captive Portal.

- 30358 – System instability may occur when applying QoS policies to SSL-VPN traffic.

- 30267 – When enabling DNS resolution in Panorama within the monitoring feature, IP addresses listed are not being resolved. Restarting the web server daemon resolved the issue. Process added to refresh DNS when updates are made to this area.

- 30144 – The country region address option is showing up in all rules. Country based addresses only work for security, SSL decryption, and DoS rules, so this option has been removed for all other rules.

- 30071 – When trying to create a custom antispyware or vulnerability signature and trying to use the "Add And" feature, only the "Add Or" feature is available. The WebUI has been updated and these functions have been separated to make it easier to add one function at a time.

- 29823 – Large core files causing disk space issues on the root partition of the firewall. Core file size limit has been reduced to prevent this issue from occurring.

- 29743 – Panorama cannot send its own hostname to a syslog server. This functionality has been added.

- 29579 – SSL decryption not working when using a wildcard certificate. In this case, the application was also using a wildcard certificate and in this situation, decryption cannot be performed. A decryption policy should be used in this case.

- 29340 – When expanding disk storage using a virtual disk in Panorama, the new virtual disk was not appearing. If a virtual disk already exists and you add a new virtual disk, you need to remove the first virtual disk before you can use the new one. Logs will be deleted when removing the initial virtual disk, so those should be backed up if they are needed. The documentation in the Palo Alto Networks Administrator's guide has been updated with this information, and the "show system disk-partition" CLI command has been added to provide more visibility to virtual disks.

- 29292 – When running the command “show system statistics vsys *vsys-number*”, no statistics are displayed. This is by design, session statistics are not VSYS specific. Show command has been updated to make it clear that you can only run system statistics for “application” on a VSYS, not sessions.

- 28938 – Request to disable HTTP TRACE method for TCP 6080 when Captive Portal is enabled on a port. Trace has been hidden in the response header.

- 28451 – If “Antivirus” and “Application and Threat” updates are scheduled to automatically update at the same time, one of the updates will fail and the system log will not update properly. Logging has been modified to identify an update that has been skipped due to a second update that is already in progress.

- 28378 – Not able to run the User Activity Report in Monitor > PDF Reports > User Activity Report because it’s being deleted before the report can be viewed. Report was only active for 30 second and has been increased to stay active for 600 seconds.

- 28361 – When in the ACC tab in the Applications section and selecting the Sessions drop down “Sort Ascending” and “Sort Descending” did not sort the column. This is by design and the drop down menu no longer shows these options.

- 25968 – High CPU on Panorama device when running a custom report to show URL categories in the last 7 days with all supported fields selected. Change made to use a summary report as the default, which allows the report to run with all fields selected.

- 25398 – When a device administrator logs into the firewall an authentication sequence is processed and one method will be used. Current logging is not identifying the authentication method that was used (LDAP, Local, AD).

- 24632 – Device administrators with read-only access are not able to export the device configuration using the WebUI. WebUI has been updated to allow this function for read-only administrators.

- 20973 – Problem exporting logs (traffic, threat) to CSV format using Firefox 3.6, which caused Firefox to stop responding. PAN-OS has been updated to support older versions of Firefox.

Known Issues

The following lists known unresolved bugs in this release:

- 33914 – In the Network tab under Global Protect > Portals/Gateways config windows, there is an “IP Address” field used for the IP of the interface for the device. You can populate this field by using the drop down for a statically assigned interface, or leave it blank for a dynamically assigned interface. In the WebUI you cannot click Ok to save the config if the IP Address field is blank.
  Workaround – Use the CLI.

- 33521 – Netflow on logical interfaces exports the IPv4 Standard template only.

- 33372 – Enabling Netflow on any interface exports flows in both directions, when it should only be sending ingress flows.

- 31688 – On devices with multiple virtual systems, the ACC may not return all data tables when switching between tabs if the tabs have a different virtual system selected in the Virtual Systems drop down.
  Workaround – Click the Submit icon (➡) once on the ACC page to refresh.

- 30444 – Exported Netflow data shows incorrect start time for some flows.

- 21601 – NetConnect may not upgrade properly from 1.1.x to 1.2 without clearing the Java cache.

- 21489 – NetConnect will not install with Java 1.5 or earlier. Java 1.6 or later is required.

- 13391 – In some environments, the threat count on the top level of ACC does not match the counts on the lower levels.

- 10800 – Connecting the PA-2000 series management port to a device that is hard set to full duplex will cause unpredictable behavior on the management port. Always set the port connected to the PA-2000 series management port to auto-negotiate.

- 7495 – CLI allows the import of more keys than the system can use.

- 5145 – Requesting an App-Scope graph for Source or Destination on a system with a very large number of sources or destinations can take 5-10 minutes to complete.

- 1985 – Using a straight cable between HA2 ports with high traffic load can lead to packet loss. When connecting HA2, use a crossover Ethernet cable.

- 1475 – Some non-browser based applications that use SSL do not function well with SSL decryption. If encountered, use an SSL Decryption rule to bypass the decryption function for these servers.

- 908 – LLC SNAP/802.2 packets do not pass through the device.

Errata

The following lists outstanding issues related to the PAN-OS documentation.

- In the File Blocking Profiles section in table 77 of the Palo Alto Networks Administrator's Guide, it states the following: *The rules are processed in sequence. To change the position of a rule, select the rule and click Move Up or Move Down*. This is not the case; the file blocking rules are not processed sequentially, so there is no need to put them in any specific order.

Related Documentation

The following additional documentation is provided:

- **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.