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.