

The controlling element for every Palo Alto Networks Next-generation firewall is PAN-OS, a modular operating system that combines three unique identification technologies (App-ID™, User-ID, Content-ID) with traditional firewall, management and networking features to restore visibility and control at the firewall, where it belongs.

PAN-OS is unique in that it performs all of its functions in a single pass. Security policy lookup, application identification and decoding, Directory services user mapping, and content scanning (viruses, spyware, IPS) are all preformed once on a given set of traffic. The single pass software brings a dramatic reduction in latency. The latest release, PAN-OS 3.1 brings significant new functionality with the key feature areas described below.

APPLICATION IDENTIFICATION FEATURES

- **Application Function Control:** The App-ID taxonomy and structure has been modified to provide a clearer method for controlling functions within applications, such as Facebook Chat within Facebook. Selecting the application within the policy will now include all functions of that application, while selecting the application function will only select the function of the application. This new structure will enable more rapid creation and deployment of policies to control individual functions.
- **Custom SSL App-ID Support:** Custom App-ID capability has been expanded to support SSL-based applications in addition to HTTP.

USER IDENTIFICATION FEATURES

- **LDAP User-ID Support:** In addition to the current Active Directory support, eDirectory and other LDAP directories are now supported by User-ID. Customers using these directory services can now deploy policies based on users and groups. For other forms of LDAP, an API for receiving IP address mapping information from external sources is also available.

CONTENT INSPECTION FEATURES

- **Custom URL Filtering Categories:** Creation of custom URL categories is now supported, enabling customers to easily address unique URL filtering requirements.
- **Custom Vulnerability Signatures:** Customers can create custom vulnerability or spyware phone home signatures on the device that can be used in the Anti-Spyware and Vulnerability Protection profiles.
- **Daily Virus Signature Releases:** The antivirus signature set is now updated on a daily basis (Monday: Friday). This means that the antivirus signatures are now upgradeable separately from the rest of the application and threat content.
- **HTML/Javascript Virus Scanning:** The antivirus engine has been enhanced to scan for HTML and Javascript viruses.

NETWORKING FEATURES

- **BGP, Jumbo Frames and PPPoE:** Dynamic routing support has been extended to support BGP (in addition to OSPF and RIP which are already supported). Jumbo frames and PPPoE are also supported in this release.
- **Policy-based Forwarding:** A new rulebase has been added to allow traffic forwarding based on policy defined by source zone/interface, source/destination address, source user/group, service, and application.
- **NAT and High Availability Enhancements:** Both NAT and HA have been enhanced to expand capacity and improve performance.

NETCONNECT SSL-VPN FEATURES

- **Expanded OS Support:** NetConnect now supports Vista 64-bit operating systems as well as Windows 7 (32- and 64-bit).
- **SecurID and CAC-based Authentication:** SecurID and CAC (Common Access Cards) can now be used with NetConnect for user authentication.
- **RADIUS VSA for Allow List:** RADIUS vendor-specific attributes can now be used to define the user allow list for SSL-VPN access.

MANAGEMENT FEATURES

- **Software, App-ID and Threat Content, and License Management via Panorama:** Panorama can now be the source for updating device software, App-ID and threat content as well as licenses.
- **SecurID Administrator Authentication:** SecurID tokens can now be used for administrators authenticating to the device or Panorama.
- **RADIUS VSAs for Admin Roles:** RADIUS vendor-specific attributes can now be used for assigning administrator roles.

VISIBILITY AND REPORTING FEATURES

- **Trace Session Tool:** When viewing the details of a log from the log viewer, all logs from other databases for that same session will also be displayed.
- **QoS Bandwidth Monitoring Tool:** A new visibility tool provides real-time visibility into application bandwidth and session consumption.
- **Admin Role for Access to User Information:** Within the role-based administration settings a new option is now available to restrict or allow access to user information within the logs, reports, and ACC.
- **Highlight Unused Rules:** From the security rulebase, there is now an option to highlight all rules that have not had a traffic match since the device booted up.
- **Multidimensional Reports:** Custom reports can now have use (nested) group-by fields to aggregate more detail into single report.
- **Hour-of-day and Day-of-week Fields:** Two new fields are available in the custom reports: hour-of-day and day-of-week allowing reports that show stats over a period of time.