APPLICATION IDENTIFICATION FEATURES

- **Custom App-IDs for Unknown Protocols:** The custom App-ID functionality has been expanded to cover unknown protocols. Applications that are currently classified as *unknowntcp* or *unknown-udp* can now be classified using custom signatures.
- **SSH Tunneling Control:** To control the use of SSH to tunnel traffic through the firewall, the decryption rulebase has been extended to support SSH. Enabling SSH decryption will allow the system to distinguish between normal shell, SCP, or SFTP access and the use of port forwarding to tunnel other traffic. Once enabled, the tunneled traffic will be classified as *ssh-tunnel* and can be controlled via security policy as needed. This is only effective for SSHv2 traffic using interactive password authentication.
- **Extended Custom App-ID Capacity:** To facilitate large scale custom App-ID classification, the capacity for custom applications has been increased. Up to 510 App-IDs can be created and shared among all virtual systems and up to 6400 virtual system-specific App-IDs can be created.
- **App and Threat Stats Collection:** A new system for anonymous collection of application and threat statistics has been added that will assist our *Application and Threat Research Center* in providing up to date analysis on the use of applications and the spread of threats. This is an opt-in service to help further the quality of application and threat coverage and will also help the team provide information back to customers relative to these statistics.
- **Identification of Dynamic Applications within an HTTP Proxy Session:** The system can now detect dynamic applications like FTP when they traverse the firewall via an HTTP CONNECT session.

USER IDENTIFICATION FEATURES

- **Windows 2003 64-bit, Windows 2008, and XenApp 6 Terminal Server Support:** The Terminal Server Agent used for identifying and controlling user traffic from a shared Citrix or Microsoft Terminal Server now support 64-bit operating systems in addition to the already supported 32- bit versions.
- **CAC and Client Certificates for Captive Portal:** CAC and client certificate support for authentication has been extended to captive portal configurations.
- **Authentication Sequences:** To facilitate authentication in environments where users or admins may reside in multiple directories or directory types, *Authentication Profiles* can now be grouped into an *Authentication Sequence* so that the system will attempt to find the user or admin in each one successively.
- **Kerberos Authentication:** Kerberos is now available as an *Authentication Profile* type and can be used anywhere *Authentication Profiles* are used.
- **Strip X-Forwarded-For Headers:** The system now has an option to mask any *X-Forwarded-For* headers that are present in outbound HTTP requests so that internal network details inserted by proxies are not exposed to the outside network.
- **Destination Port in Captive Portal Rules:** A new field for destination port has been added to the captive portal rulebase to allow control over which ports can leverage the captive portal feature by intercepting HTTP requests for unknown users.

CONTENT INSPECTION FEATURES

- **Behavior-based Botnet Detection:** Leveraging ongoing research by the *Application and Threat Research* team as they add signatures for known botnets, a new report has been added that provides scores for hosts on the network that appear to be part of a botnet.
- **Drive-by-Download Protection:** To prevent unintentional or malicious download of executable files, a continue page option has been added to the *File Blocking Profile.* This can be used to prevent users from accidental downloads as well as prevent malicious scripts or malware from using HTTP to download files to internal systems.
- **Container Page Logging:** To provide more focused URL filtering logs, a new capability to identify container pages and optionally only log container pages, skipping images, stylesheets, javascript files, etc. has been added.
- **Extended URL Logging:** URL logs will now record up to 1023 bytes of each requested URL.
- **DoS Protection Rulebase:** Complementing the existing *Zone Protection Profiles*, a new Denial of Service rulebase and corresponding *DoS Protection Profile* have been added to provide more granular and proactive protection from DoS attacks.

- **Combination Custom IPS Signatures:** When creating custom vulnerability signatures, multiple existing signatures can be combined together along with frequency to provide visibility into and protection from multi-stage attacks.
- **Hold-down Time Scan Detection:** New reconnaissance protection options have been added to block the source for a specified period of time. Thresholds can be set to track by source or by source and destination pair.
- **PDF Virus Scanning:** Support for detection of virus infected PDF files has been added to the antivirus engine.
- **Out-of-Band URL Database Update:** In addition to the automated database updates, the URL database can now be updated manually via SCP or TFTP via the CLI.

NETWORKING FEATURES

- **Active/Active HA:** To better support asymmetrically routed environments, two devices can be deployed in an HA configuration with either virtual wire interfaces or layer 3 interfaces. App- ID and Content-ID are fully supported in asymmetric environments by providing a new HA3 interface allowing a given session to be handled by a single device for layer 7 inspection. A/A also incorporates flexible layer 3 deployment options supporting load-sharing and interface IP failover.
- **HA Enhancements:** Several enhancements have been made to the HA functionality:
    - Link Failover
    - Next-hop Gateway for HA1 Interface
    - HA Port Configurability for PA-4000 Series
    - Backup HA Interface
    - Layer 3 HA2 Support
- **IPv6 Support on L2 and L3 Interfaces:** In addition to the IPv6 support available on virtual wire configurations, the system now supports IPv6 in layer 2 and layer 3 configurations.
- **Country-based Policy Enforcement:** Source and destination country can now be used in policy. In addition, custom regions can be created to map internal addresses or to override the country mapping of a current mapped IP address. The IP mapping database is now updated on a weekly basis as part of the application and threat content release.
- **VR to VR Routing:** Another virtual router can now be specified as the next hop when creating static routes.
- **Virtual System as Destination in PBF Rule:** A virtual system can now be specified as the next hop in a policy-based forwarding rule.
- **DNS Proxy:** DNS proxy can now be enabled on an interface to provide rule-based DNS resolution (e.g. resolving internal hosts with an internal DNS server while resolving all other requests with an external DNS). In addition, static entries can be added to the proxy configuration. A DNS proxy can also be used for management services in place of an explicitly configured DNS server.
- **Virtual System Resource Control:** Many additional controls have been added to restrict the capacities allowed to be consumed by a given virtual system.
- **Overlapping IP Address Support:** To facilitate shared use of a device, the system now supports the use of the devices layer 3 services for clients that have the same IP address of interfaces or hosts in another virtual router.
- **Untagged Subinterfaces:** Multiple untagged layer 3 interfaces can now be created on a single physical interface. The source interface will be determined based on the destination IP address as opposed to a VLAN tag.
- **TCP MSS Adjustment:** TCP MSS adjustment can now be enabled on an L3 interface.
- **Source Port Filtering:** Service objects now have source port as an option field that can be specified in order to control traffic based on source port.

GLOBALPROTECT FEATURES

- GlobalProtect is a new system for protecting users and corporate assets when users roam off of the protected corporate network. Using GlobalProtect, roaming devices will discover the nearest PAN-OS gateway and have the benefit of all of the application and user-based policies as well as the complete threat prevention and URL filtering. GlobalProtect requires a Portal license for the overall system and a Gateway license on each firewall that will be participating in the distributed enforcement.
    - **Network Discovery and Auto-Connection:** The GlobalProtect client supports automatic network discovery to determine when the user is off the corporate network and autoconnection to the nearest gateway for seamless, unobtrusive connection setup and scanning.
    - **Host Profiling:** In addition to the existing matching criteria, information about the host state can now be used in policy through *Host Information Profiles.*
    - **Windows XP, Vista, 7 Support:** GlobalProtect is now available for Windows XP, Vista, and Windows 7 both 32- and 64-bit versions.
    - **Single Sign-On Support:** GlobalProtect can leverage existing Windows login processes.

NETCONNECT SSL-VPN FEATURES

- **Password Expiration Notification:** A new option for notifying users of impending password expiration can be enabled for NetConnect and GlobalProtect users.
- **Proxy ARP Support:** For SSL-VPN and GlobalProtect configurations, the system will now perform a proxy ARP function for the IP addresses that it gives out to remote clients.
- **VPNs using PPPoE Interfaces:** PPPoE interfaces with statically assigned addresses can now be used in SSL-VPN and GlobalProtect configurations.

MANAGEMENT FEATURES

- **New UI Architecture:** A new user interface framework has been introduced that allows for a much richer user experience. There are many benefits with the new framework including the following:
    - Drag and drop for policy editing and rule reordering
    - Pop-up menu to see object values in policy view
    - Searching and filtering throughout the interface, including free text search
    - Customizable table layouts
    - Integrated object creation and editing within the policy context

- **Rule Tagging:** To facilitate categorization and quick filtering of rules, tagging has been introduced.
- **Object Descriptions:** Address and service objects now have a description field.
- **FQDN-based Address Objects:** A fully qualified domain name can now be used for address object definition. The system will resolve the name at runtime and store up to 10 addresses for a given name. The addresses will be refreshed based on the TTL values returned by DNS.
- **Configurable Log Storage by Type:** The storage allocation for logs and packet captures can be customized.
- **Configurable Log Formats:** The format of logs generated via syslog and email can now be customized.
- **ArcSight CEF Format:** The system now support the ArcSight CEF format using the configurable log formatting function.
- **Configuration Transactions:** To facilitate multi-administrator workflow, configuration and commit transaction locking mechanisms have been introduced. Commit locking can be enabled automatically or on demand when performing complex, multi-stage configuration changes to avoiding commit of partial configurations.
- **SNMPv3 Support:** SNMPv3 is now supported for monitoring as well as log forwarding.
- **Extended Virtual System Reporting:** Virtual system administrators now have access to the scheduling and email forwarding capabilities of the custom reporting function.
- **UI-based PCAP Configuration:** Administrators can now configure and access the packet capture functionality via the web interface.

PANORAMA FEATURES

- **Extended Object Sharing:** Additional sharing of configuration across multiple devices and virtual systems is now available. All rulebases are now available within Panorama and all policy objects can be configured and shared within a device group for use in device-specific policy. In addition, the server, log forwarding and authentication profiles as well as local users and groups are now shareable to devices and virtual systems within a device group.
- **NFS-based Log Storage:** An external NFS mount may now be used for extended log storage.
- **High Availability:** Panorama can now be deployed with two instances in a redundant configuration for high availability. Each Panorama requires a dedicated license.
- **Local Log Buffering:** When the connection between a device and Panorama is recovered after being lost, the device will forward any logs that were generated while disconnected.
- **User Activity Report:** The *User Activity Report* is now available within Panorama, reporting on the data collected in the Panorama databases.
- **Exportable Config Backups:** A complete bundle of all of the current configurations of all managed devices and Panorama can now be downloaded as a single TGZ file. In addition, the system can be configured to export this bundle automatically to an external FTP server on a nightly basis.
- **Comprehensive Config Audit:** A new configuration auditing report has been added to show all relevant changes that would occur when doing a *Commit All* from within Panorama. This includes local device changes as well as any shared configuration changes from within Panorama. This will generate an HTML file that can be archived or emailed for review.