What’s New in PAN-OS 5.0

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.