krome

paloalto NETWORKS®

Whats New in Palo Alto Networks PAN-OS 7.1

Palo Alto Networks expands its Next Generation Security Platforms prevention capabilities with the release of PAN-OS 7.1. The new features in this release improve attack prevention, in more deployments, even faster than before, preventing breaches before they can occur, no matter the location. Here is a summary of the new features in PAN-OS 7.1.

Management Features

- **Commit Queues** - The firewall and Panorama™ now queue commit operations so that you can initiate a new commit while a previous commit is still in progress. This enables you to activate configuration changes without having to coordinate commit times with other administrators. For example, after reconfiguring a firewall locally, you can initiate a firewall commit while it is still receiving device group and template settings that a Panorama administrator committed. In Panorama, you can also initiate a single commit to push settings from multiple device groups that target different virtual systems on the same firewall instead of committing from one device group at a time.
- **Synchronisation of SNMP Trap and MIB Information** - When an event triggers SNMP trap generation (for example, an interface goes down), the firewall, Panorama virtual appliance, M-Series appliance, and WF-500 appliance now update the corresponding SNMP object in response (for example, the interfaces MIB) instead of waiting for the 10-second timer to expire and allowing SNMP queries to receive out-of-sync replies. This ensures that your network management system displays the latest information when polling an object to confirm the event.
- **Banners and Message of the Day** - For the firewall and Panorama, you can now customise the web interface as follows:
    - » Force administrators to acknowledge the login banner to ensure they see information they need to know before they log in, such as login instructions.
    - » Add a message of the day that displays in a dialog after administrators log in to ensure they see important information, such as an impending system restart, that can affect their tasks. The same dialog also displays messages that Palo Alto Networks embeds to highlight important information associated with a software or content release.
    - » Add colored bands that highlight overlaid text across the top (header banner) and bottom (footer banner) of the web interface to ensure administrators see critical information, such as the classification level for firewall administration.
- **Support for Certificates Generated with 4,096-bit RSA Keys** - The firewall and Panorama now support certificates generated with 4,096-bit RSA keys, which are more secure than smaller keys. You can use these certificates to authenticate clients, servers, users, and devices in several applications, including SSL/TLS decryption, Captive Portal, GlobalProtect™, site-to-site IPSec VPN, and web interface access.
- **Bootstrapping Firewalls for Rapid Deployment** - For agility and efficiency in deploying the Palo Alto Networks next-generation firewall at a remote site or at a data center, you can now fully provision (bootstrap) a firewall with or without Internet access. Bootstrapping reduces operational effort and service-ready time by eliminating manual configuration steps and user errors when deploying new firewalls. You can now bootstrap the firewall using an external device—a USB flash drive or a virtual CD ROM/DVD—and accelerate the process of configuring and licensing the firewall. The bootstrapping process is supported on all hardware-based firewalls and on VM-Series firewalls in both the private cloud (KVM, ESXi, Hyper-V) and the public cloud (AWS, Azure).

Whats New in Palo Alto Networks PAN-OS 7.1

- **Web Interface Design Refresh** - The web interface design on Panorama and the firewalls is redesigned with new icons and buttons and an updated font and color scheme. This modernisation does not include any changes in layout or workflows to ensure that you do not need to re-familiarise yourself with the user interface.
- **New API Request to Show PAN-OS Version** - You can now use the PAN-OS XML API to show the PAN-OS version on a firewall or Panorama. In addition to the PAN-OS version, this new API request type (type=version) provides a direct way to obtain the serial number and model number.
- **Unified Logs** - A new unified log view allows you to view the latest Traffic, Threat, URL Filtering, WildFire™ Submissions, and Data Filtering logs on a single page. While the individual log views are still available for these log types, the unified log view enables you to investigate and filter these different types of logs in a single view. Unified logs also allows you to perform a search from AutoFocus to a targeted firewall or Panorama. Learn more about how to use AutoFocus with a firewall or Panorama.
- **AutoFocus™ and PAN-OS Integrated Logs** - AutoFocus threat intelligence data is now integrated with PAN-OS logs, providing you with a global context for individual event logs. You can now click on an IP address, URL, user agent, filename, or hash in a PAN-OS log entry to display an AutoFocus threat intelligence summary of the latest findings and statistics for that artifact. Use the new AutoFocus summary for log entry artifacts to quickly assess the pervasiveness and risk of an artifact while still in the firewall or Panorama context. You can then open an expanded AutoFocus search directly from the firewall or Panorama.
- **Administrator Login Activity Indicators** - To detect misuse and prevent exploitation of administrator accounts on a Palo Alto Networks firewall or Panorama, the web interface and the command line interface (CLI) now display the last login time and any failed login attempts when an administrator logs in to the interface. These administrator login activity indicators allow you to easily identify whether someone is using your administrative credentials to launch an attack.

Virtualisation Features

- **VM-Series Firewall for Microsoft Azure** - The VM-Series firewall can now be deployed in Azure, the Microsoft public cloud. The VM-Series firewall can be deployed as a gateway that secures and integrates your multi-tier applications and services in the Azure cloud and the corporate office or enterprise data center, and as a next-generation firewall that secures inter-application traffic within the Azure cloud. Both the bring your own license (BYOL) model and the hourly pay-as-you-go (PAYG) model of the VM-Series firewall are available in the Azure Marketplace.
- **Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall** - When using the VM-Series NSX edition solution for automated provisioning of VM-Series firewalls, you can now create multiple service definitions on Panorama. You can now have separate Security policy rules for VM-Series firewalls deployed on different ESXi clusters but managed by a vCenter Server and NSX Manager. This capability allows you to define tenant-specific Security policy rules for securing guest virtual machines within an ESXi cluster. Each service definition (up to 32 are supported) includes a template, a device group, and the license auth codes for firewalls deployed using this service definition. Additionally, you can configure Access Domains on Panorama to limit administrative access to a specified set of firewalls.
    - » The VM-Series firewall now also supports multiple zones and virtual wire interface pairs, allowing you to create zone-based policy rules with a single (common) set of Security policy rules for guest virtual machines that belong to different tenants or departments; traffic separation is made possible by allocating a unique zone and pair of virtual wire interfaces for guest virtual machines that belong to a specific tenant or department. This capability also allows you to enforce policy on guest virtual machines that have overlapping IP addresses, typically seen in cases where the guest virtual machines are assigned to separate VLANs, VXLANs, or Security groups in the vSphere environment.
- **VM-Series Firewall for Microsoft Hyper-V** - To expand support for deploying the VM-Series firewall in private cloud and hybrid cloud environments, you can now deploy the VM-Series firewall on Hyper-V Server 2012 R2 (standalone edition) or Windows Server 2012 R2 (standard and datacenter editions) with the Hyper-V role that lets you create and manage virtual machines. You can deploy one or more instances of the VM-Series firewall using the Hyper-V Manager (guided user interface) or Windows PowerShell (command line interface). Tap, virtual wire, Layer 2, and Layer 3 interface modes are supported.

- **Support for VMware Tools on Panorama and on VM-Series Firewalls on ESXi** - For ease of administration, the VM-Series firewall and the Panorama virtual appliance are now bundled with a customised version of open-vm-tools. This bundle allows the virtual infrastructure administrator to:
  - » View the management IP address and PAN-OS version of the firewall and Panorama on vCenter.
  - » View resource utilisation metrics for the hard disk, memory, and CPU.
  - » Monitor availability and health status of the virtual appliance using a heartbeat mechanism.
  - » Gracefully shutdown and restart the firewall and Panorama from the vCenter server.
- **Support for Device Group Hierarchy in the VM-Series NSX Edition Firewall** - With this enhancement, you can now assign the VM-Series NSX edition firewall to a template stack and a device group in a hierarchy so that the firewalls can inherit settings defined in the stack and the hierarchy. As you provision or power off virtual machines in the vSphere environment, you can enable notification of IP address changes to one or more device groups in a hierarchy. This notification allows Security policy rules that reference Dynamic Address Groups to collect information on the changes and dynamically drive policy updates to secure the network.
- **Support for Synchronising VM Monitoring Information on Firewalls in HA** - For a pair of firewalls (VM-Series and hardware-based firewalls) deployed in a high availability configuration, dynamic data such as information about virtual machine IP addresses and other monitored attributes, can now be synchronised between HA peers.
- **Support for Amazon ELB on the VM-Series Firewalls in AWS** - To use Amazon Elastic Load Balancing (ELB) for increased fault tolerance in your AWS deployment, the primary interface (management) on the VM-Series firewall must be able to receive dataplane traffic. To integrate with the Amazon ELB, you can now swap the management interface (eth0) and dataplane interface (eth1) on the VM-Series firewall. A new CLI command (set system setting mgmt-interface-swap enable yes) allows you to swap the management interface (eth0) and dataplane interface (eth1) so that the firewall can send and receive dataplane traffic on eth0. With this change, the Amazon ELB can automatically monitor the health of the VM-Series firewalls and route traffic to healthy instances of the VM-Series firewall in the same or across Availability Zones.

Networking Features

- **Multicast Route Setup Buffering** - You can now enable buffering of the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not yet exist for the corresponding multicast group. By default, the firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. You only need to enable multicast route setup buffering only if your content servers are directly connected to the firewall and your custom application cannot withstand the first packet in the session being dropped.
- **Binding a Floating IP Address to an HA Active-Primary Firewall** - In an HA active/active deployment, you can now bind a floating IP address to the firewall in the active-primary state. Thus, on a failover, when the active-primary firewall (Peer A) goes down and the active-secondary firewall (Peer B) takes over as the active-primary peer, the floating IP address moves to Peer B. Traffic continues to go to Peer B, even when Peer A recovers and becomes the active-secondary device. This feature provides more control over how floating IP address ownership is determined as firewalls move between HA states. Prior to this feature, the floating IP address was bound to the firewall through its Device ID [0/1] and would follow the Device ID to which it was bound. Now, in mission-critical data centers, you can benefit from this feature in several ways:
  - » You can have an active/active deployment so that you can do path monitoring out of both firewalls, yet the HA peers function like an active/passive deployment because traffic directed to the floating IP address always goes to the active-primary firewall.
  - » The floating IP address does not move back and forth between HA devices if the active-secondary device flaps up and down. Therefore, traffic remains stable on the active-primary firewall.
  - » You have control over which firewall owns the floating IP address, so you can keep new and existing sessions on the active-primary firewall.
  - » You can verify a firewall is fully functional before you manually pass ownership of the floating IP address back to it.

Whats New in Palo Alto Networks PAN-OS 7.1

- **Per VLAN Spanning Tree (PVST+) BPDU Rewrite** - When an interface on the firewall is configured for a Layer 2 deployment, the firewall now rewrites the inbound Port VLAN ID (PVID) number in a Cisco per-VLAN spanning tree (PVST+) bridge protocol data unit (BPDU) to the proper outbound VLAN ID number and forwards it out. This new default behavior in PAN-OS 7.1 allows the firewall to correctly tag Cisco proprietary Per VLAN Spanning Tree (PVST+) and Rapid PVST+ frames between Cisco switches in VLANs on either side of the firewall. Thus, spanning tree loop detection using Cisco PVST+ functions properly. There is no behavior change for other types of spanning tree.
- **Configurable MSS Adjustment Size** - The Maximum Segment Size (MSS) adjustment size is now configurable so that you can adjust the number of bytes available for the IP and TCP headers in an Ethernet frame. You can expand the adjustment size beyond 40 bytes to accommodate longer IP and TCP headers. For example, if you are forwarding a packet through an MPLS network where multiple tags can be added to the packet, you may need to increase the number of bytes in the header.
- **DHCP Client Support on the Management Interface** - The management interface on the firewall now supports DHCP client for IPv4, which allows the management interface to receive its IPv4 address from a DHCP server. The management interface also supports DHCP Option 12 and Option 61, which allow the firewall to send its hostname and client identifier, respectively, to a DHCP server.
- **Increase in Number of DHCP Servers per DHCP Relay Agent** - In a DHCP relay agent configuration, each Layer 3 Ethernet or VLAN interface now supports up to eight IPv4 DHCP severs and eight IPv6 DHCP servers. This is an increase over the previous limit of four DHCP servers per interface per IP address family.
- **PA-3000 Series and PA-500 Firewall Capacity Increases** - PA-3000 Series and PA-500 firewalls support more ARP entries, MAC addresses, and IPv6 neighbors than they supported in prior releases. Additionally, PA-3000 Series firewalls support more FIB addresses. The new capacities are listed in the New Features Guide.
- **SSL/SSH Session End Reasons** - The Session End Reason column in Traffic logs now indicates the reason for SSL/SSH session termination. For example, the column might indicate that a server certificate expired if you configured certificate expiration as a blocking condition for SSL Forward Proxy decryption. You can use SSL/SSH session end reasons to troubleshoot access issues for internal users requesting external services or for external users requesting internal services.
- **Fast Identification and Mitigation of Sessions that Overutilise the Packet Buffer** - A new CLI command (show running resource-monitor ingress-backlogs) on any hardware-based firewall platform allows you to see the packet buffer percentage used, the top five sessions using more than two percent of the packet buffers, and the source IP addresses associated with those sessions. This information is very helpful when a firewall exhibits signs of resource depletion and starts buffering inbound packets because it is an indication that the firewall might be experiencing an attack. Another new CLI command (request session-discard [timeout <x>] [reason <reason_string>] id <session_id>) allows you to immediately discard a session without a commit.

App-ID Features

- **PDF Report for Visibility into SaaS Applications** - The new SaaS application usage PDF report provides visibility into the SaaS applications in use on your network. SaaS is a way of delivering applications where the service provider owns and manages the software and the infrastructure, and the user controls the data, including the rights to who can create, access, share, and transfer data.
    - » The new report helps you identify the ratio of sanctioned versus unsanctioned SaaS applications in use on the network and includes details on the top SaaS application subcategories by number of applications, by number of users, and by volume of data transferred using these applications.
    - » The key findings in this report summarise how your SaaS application usage compares to most Palo Alto Networks customers and the percentage of your users who use one or more unsanctioned SaaS applications. You can use the data from this report to define or refine security policy rules on the firewall to block or monitor the use of unsanctioned SaaS applications on your network.

Whats New in Palo Alto Networks PAN-OS 7.1

Content Inspection Features

- **Protection Against LZMA Compressed Adobe Flash Files** - The firewall now supports hash-based protection against malicious Adobe flash files that have undergone Lempel-Ziv-Markov chain algorithm (LZMA) compression. Though LZMA compression is a legitimate type of compression that allows data to be reconstructed in its original form without data loss, it can also be used to compress malicious files so that they evade detection.
- **Extended Support for URLs and Domain Names in an External Dynamic List** - External Dynamic Lists (formerly called Dynamic Block Lists) now support URLs and domain names in addition to IP addresses. External dynamic lists allow you to automate and simplify the process of importing URLs, domain names, and IP addresses into the firewall. These lists allow you to take prompt action when you receive threat intelligence from external sources because they do not require a configuration change or commit on the firewall. For domains, you can configure the firewall to alert, block, or sinkhole traffic when performing a DNS resolution. For URLs, you can trigger an alert or block the traffic when the user makes an HTTP request. IP address lists continue to be available for use in policy rules and are best suited for enforcing an IP block list.
- **Each External Dynamic List can include entries of one type only** - IP address, URL, or domain. You cannot combine different types of entries in a single list.
- **TCP Sessions and Content-IDTM Settings in the Web Interface.** - Now, all of the settings required to protect your network from Layer 4 and Layer 7 evasions are available in the web interface for simplified configuration. These settings were previously only available from the CLI.

User-ID Features

- **User-ID Redistribution Enhancement** - You can now relay user mapping information from one firewall to another in a sequence of up to ten firewalls instead of two. This increase in the relay sequence enables you to redistribute mapping information in a network that has hundreds of user identification sources or that has users who rely on local sources for authentication (for example, regional directory services) but who need access to remote resources (for example, global data center applications).
- **Ignore User List Configurable in Web Interface** - For the PAN-OS integrated User-ID agent, you can now use the firewall web interface as an alternative to the CLI to configure the ignore user list, which specifies the user accounts that don't require IP address-to-username mapping (for example, kiosk accounts). Using the web interface is easier and reduces the chance of errors that might compromise the enforcement of user-based policies.
- **User Group Capacity Increase** - PA-5060 and PA-7000 Series firewalls that have the multiple virtual systems capability disabled can now base policies on up to 3,200 distinct user groups instead of 640. This ensures continued security on networks that use a large number of groups to control access to resources.

WildFire Features

- **5 Minute WildFire Updates** - The WildFire public cloud now globally distributes virus and DNS signatures every five minutes to Palo Alto Networks firewalls. This quick distribution enables firewalls with a WildFire subscription to detect and block threats within minutes of discovery. With earlier PAN-OS release versions, WildFire updates are made available every fifteen minutes.
- **New WildFire API Features** - You can now use the WildFire API to submit links for WildFire analysis and to get verdicts for samples. These new WildFire API features are supported both with the WildFire public cloud and on a WildFire private cloud.

Decryption Features

- **Transparent Certificate Distribution for SSL Forward Proxy** - You can now use GlobalProtect to easily distribute the forward trust certificate required for SSL Forward Proxy decryption to client systems.
- **Perfect Forward Secrecy (PFS) Support with SSL Forward Proxy Decryption** - PAN firewalls now support PFS when performing SSL Forward Proxy decryption. PFS ensures that data from the session undergoing SSL Forward Proxy decryption cannot later be retrieved in the event that server private keys are compromised. You can enforce Diffie-Hellman key exchange-based PFS (DHE) and/or elliptic curve Diffie-Hellman-based PFS (ECDHE) with SSL Forward Proxy.

Whats New in Palo Alto Networks PAN-OS 7.1

VPN Features

- **DES Support for Crypto Profiles** - IKE gateways and IPSec tunnels now support Data Encryption Standard (DES) as an encryption algorithm in crypto profiles for a site-to-site VPN connection. DES support provides backward compatibility with legacy devices that do not use stronger encryption methods.

GlobalProtect Features

- **GlobalProtect App for Chrome OS** - The new GlobalProtect app for Chrome OS is now available for Chromebooks running Chrome OS 45 and later. The app, which is available from the Chrome Web Store, extends the same next-generation firewall-based policies that are enforced within the physical perimeter to devices running Chrome OS. GlobalProtect portals and gateways support the GlobalProtect app for Chromebooks in PAN-OS 6.1 and later releases.
- **Simplified GlobalProtect Agent User Interface for Windows and Mac OS Clients** - The GlobalProtect agent 3.0 for Windows and Mac OS now displays a simpler, cleaner user interface. As part of the redesign, a user can now log in to the GlobalProtect portal and view connection status information right from the main Home tab. The remaining tabs provide details and statistics about the connection, information that the GlobalProtect agent is collecting about the host state, and troubleshooting information.
- **Dynamic GlobalProtect App Customisation** - New app configuration options for the GlobalProtect will now be available with content releases. This change will allow you to take advantage of new app configuration features without waiting for the next PAN-OS release.
    - » With this feature, you can also view all customisation options from the new App tab in a GlobalProtect portal agent configuration. Configure these options to change the default display of the GlobalProtect user interface, usability preferences, timeout values, and scenario-based behaviors.
    - » Included in the new customisation options are settings that, in earlier releases, required you to define their values in the Windows registry or Mac global property list (plist). Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows registry or the Mac plist.
- **Enhanced Two-Factor Authentication for GlobalProtect** - Two-factor authentication is now easier to deploy and use. By deploying a client certificate through the Simple Certificate Enrollment Protocol (SCEP) and by enabling dynamic passwords, such as one-time passwords (OTPs), you make strong two-factor authentication easier, as follows:
- **Client certificate distribution** - For easier deployment, the GlobalProtect portal can now request a client certificate from your enterprise public key infrastructure (PKI) and issue the certificate to a user—without exposing the PKI infrastructure to the Internet. The client certificate has a configurable lifespan, typically 90 days. GlobalProtect automates the process by using SCEP to obtain and install certificates transparently, thus simplifying the deployment of credentials.
- **Cookie authentication** - To reduce the number of times users must enter their two-factor authentication credentials, you can now configure GlobalProtect to require users to log in only once when connecting to GlobalProtect portals and gateways. After a user authenticates and connects, GlobalProtect creates an encrypted cookie and issues it to the GlobalProtect agent. With an encrypted cookie on their device, users can remain logged in for the lifespan of the cookie (typically 24 hours). For each subsequent login during the lifespan of the cookie (for example, after the device wakes up from the sleep state), GlobalProtect uses the cookie to authenticate the user instead of requiring the user to enter credentials.
- **Client Authentication Configuration by Operating System or Browser** - For increased flexibility, you can now specify the client operating system (Android, iOS, Windows, Mac, or Chrome), to which to apply a client authentication configuration. You can also customise the client authentication for satellite devices, web-based browser access (GlobalProtect portal only), and third-party IPSec VPN access (GlobalProtect gateways only). This enhancement enables you to customise the authentication method for different sets of users.
- **Kerberos Single Sign-On for GlobalProtect** - GlobalProtect clients running on Windows 7, 8, or 10 now support Kerberos V5 single sign-on (SSO) for GlobalProtect portal and gateway authentication. In this implementation, the GlobalProtect portal and gateway act as Kerberos service principals, and the GlobalProtect app acts as a user principal and authenticates the user with a Kerberos service ticket from the Key Distribution Center (KDC). Kerberos SSO is primarily intended for internal gateway deployments to provide accurate User-IDTM information transparently without any user interaction.

Whats New in Palo Alto Networks PAN-OS 7.1

- **Customisable Password Expiry Notification Message** - You can now customise the notification message that GlobalProtect displays when a user's password is about to expire. The new option is available in the GlobalProtect portal agent configuration and is supported using the LDAP authentication method. The GlobalProtect agent appends the custom message to the standard password expiry notification message that it displays before a user's password expires. This enhancement enables you to display information that users may need when their password is about to expire.
- **Enhanced Authentication Challenge Support for Android and iOS Devices** - GlobalProtect for iOS and Android devices now supports two-factor authentication challenge as a one-time password (OTP). When prompted, the user can now cancel the login to view the token password sent via SMS or using any other token retrieval app on the mobile device. The user must then return to the GlobalProtect app and log in with the valid token password within 30 seconds. If the user does not successfully enter the password within 30 seconds, the authentication challenge disappears and the user must restart the GlobalProtect app to enter the password.
- **Block Access from Lost or Stolen and Unknown Devices** - For greater protection against unauthorised network access, you can now block access from known and unknown devices. To block network access from known devices, you can now add host IDs to a device block list. This is useful when a user reports that a device is lost or stolen and you need to take immediate action.
    - » To prevent unauthorised access from unknown devices, you can now configure the firewall to pre-deploy client certificates through the Simple Certificate Enrollment Protocol (SCEP) and enable GlobalProtect to use the SCEP configuration on Palo Alto Networks firewalls to validate that these client certificates (used to authenticate users) were positively issued to the authenticating device. When enabled, GlobalProtect blocks the session if the certificate does not match the device to which the certificate was issued. Both methods offer greater protection against unauthorised network access from known and unknown devices.
- **Certificate Selection by OID** - You can now specify the certificate that GlobalProtect uses for authentication on Windows and Mac clients by entering the certificate object identifier (OID). By specifying the OID, GlobalProtect filters out all other certificates except for those with the matching OID.
- **Save Username Only Option** - You can now enable GlobalProtect to save only a username when users log in to GlobalProtect. The new option improves provides an alternative to saving both the username and password.
- **Use Address Objects in a GlobalProtect Gateway Client Configuration** - You can now use an address object, which can include an IPv4 address (single IP address, range, or subnet) or an FQDN, when configuring IP address pools or access routes in a GlobalProtect gateway client configuration. You can also define address objects in Panorama and deploy them with GlobalProtect settings to gateway devices.
- **Transparent Distribution of Trusted Root CAs for SSL Decryption** - You can now easily and transparently install the trusted root certificate authority (CA) certificates required for SSL forward proxy decryption in a GlobalProtect portal configuration. For each CA certificate that you enable, the GlobalProtect portal automatically distributes the certificate to the GlobalProtect agent which installs it in the certificate store on GlobalProtect endpoints. The firewall uses these certificates to establish itself as a trusted third party to the session between the client and the server.
- **Maximum Internal Gateway Connection Retry Attempts** - You can now configure the maximum number of retries when the GlobalProtect agent fails to connect to an internal gateway. By default, the agent does not retry the connection attempt when the internal gateway is temporarily down or unreachable. With this new feature, you can specify the number of retries by configuring the option in a GlobalProtect portal agent configuration.
- **GlobalProtect Notification Suppression** - You can now suppress the bubble notification that GlobalProtect displays from the notification area (system tray). Each notification contains information about changes in the agent status. Suppressing the bubble notification allows the GlobalProtect agent to run more transparently and enables you to further customise the behavior of the GlobalProtect agent that runs on Windows clients.
- **Disable GlobalProtect Without Comment** - For increased flexibility, you can now allow a user to disable the GlobalProtect app without providing a comment, passcode, or ticket number. In this release, you can configure the option as part of a GlobalProtect portal agent configuration. In earlier releases, this option was only available in the Windows registry or Mac global property list (plist). Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows registry or the Mac plist.

Whats New in Palo Alto Networks PAN-OS 7.1

Panorama Features

- **Role Privileges for Commit Types** - For custom Panorama administrator roles, you can now assign commit privileges by type (Panorama, device group, template, or Collector Group) instead of assigning one comprehensive commit privilege. This improves the security of Panorama, firewalls, and Log Collectors by providing more granular control over the types of configuration changes that each Panorama administrator can commit.
- **8TB Disk Support on the Panorama Virtual Appliance** - You can now add a virtual disk of up to 8TB instead of 2TB on a Panorama virtual appliance that runs on a VMware ESXi server (version 5.5 or later) or on vCloud Air. This increased disk capacity enables Panorama to store more logs.

AutoFocus Features

- **AutoFocus Remote Search** - In AutoFocus, you can now remotely search for suspicious IP addresses, hashes, URLs, user agents, and filenames on a targeted firewall. The AutoFocus remote search then opens the firewall web interface to the unified log view so that all firewall log entries with the suspicious artifacts are collectively displayed.
  - » This feature is one of three features introduced in PAN-OS 7.1 that supports integration between a firewall or Panorama and AutoFocus. For more details on these features, and how they complement each other, see the PAN-OS and AutoFocus Integrated Features Quick Start Guide.

Hardware Features

- **PA-7000 Series Firewall Network Processing Cards with Double the Session Capacity** - Two new Network Processing Cards (NPCs) are now available to double the session capacity of previously released NPCs.
  - » PA-7000-20GXM—Doubles the memory of the PA-7000-20G NPC, enabling support for eight million sessions (up from four million). This NPC has twelve RJ-45 10/100/1000Mbps ports, eight SFP ports, and four SFP+ ports.
  - » PA-7000-20GQXM—Doubles the memory of the PA-7000-20GQ NPC, enabling support for eight million sessions (up from four million). This NPC has twelve SFP+ ports and two QSFP ports.

For example, installing ten PA-7000-20GXM NPCs in a PA-7080 firewall enables support for up to 80 million sessions. All PA-7000 Series NPCs are compatible with each other, so you can install any combination of them in a PA-7050 or PA-7080 firewall.

Note: You must upgrade the firewall to PAN-OS 7.1 before you install a PA-7000-20GXM or PA-7000-20GQXM NPC.

For more information you can also refer to the PA-7000 Series Hardware Reference Guide.

Find Out More

If you would like to discuss how your organisation could benefit from Palo Alto Networks Security solutions please do get in touch with one of our Business Managers, we'd love to share our experiences, and help you to plan and deliver your Next-Generation Security platform.

Telephone: +44 (0) 1932 232345
Email: info@krome.co.uk
Web: www.krome.co.uk