CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0.5

Maintenance Report Number: CCEVS-VR-VID11063-2021-2

Date of Activity: 30 June 2021

References: Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." March 20, 2013

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004

Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS10.0.5 Security Target, Version 1.0, June 1, 2021

Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Firewalls with PAN-OS 10.0 Revision Date: June 1, 2021

Palo Alto Networks PA-220 Series, PA-800 Series, PA- 3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next- Generation Firewall with PAN-OS 10.0.5 Impact Analysis Report, Version 1.0, June 1, 2021

Description of Changes

The changes made to the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0 since the previous Common Criteria assurance maintenance update in April 2021 (CCEVS-VR-VID11063-2021) are described here.

- The PA-3000 Series (PA-3020, PA-3050, PA-3060) Firewalls have reached End-of-Life and are no longer considered part of the evaluated configuration.
- The Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall was updated from version PAN-OS 9.1.8 to version PAN-OS 10.0.5. The software updates included new non-security relevant features and bug fixes. The software updates and their effects and relevance are summarized below.
- Support for the optional Palo Alto PA-7000-DPC-A Network Processing Card has been added to the evaluation.

The PAN-OS release notes from PAN-OS 10.0.0 to PAN-OS 10.0.5 include updates from the Palo Alto Networks next-generation firewalls, Panorama, and Wildfire product lines. All three of these product lines implement PAN-OS and Palo Alto has included all in a release note format. The following product updates are applicable to the PAN-OS 10.0.5 firewalls.

Features Introduced in PAN-OS 10.0

Feature	Description	Rationale
Enterprise Data Loss Prevention (DLP)	To protect against unauthorized access, misuse, extraction, and sharing of sensitive information, you need to effectively filter network traffic to block or generate an alert before sensitive information leaves the network. Enterprise Data Loss Prevention (DLP) provides a single engine for accurate detection and consistent policy enforcement for sensitive data at rest and in motion. Panorama and managed firewalls running PAN-OS 10.0.2 and later releases support Enterprise DLP.	**Minor Change –** Data Loss Prevention (DLP) was excluded from the v9.0 evaluation and is excluded from the 10.0.5 release also. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
IoT Security Features IoT Security	The IoT Security solution works with next-generation firewalls to dynamically discover and maintain a real-time inventory of the IoT devices on your network. Through AI and machine-learning algorithms, the IoT Security solution achieves a high level of accuracy, even classifying IoT device types encountered for the first time. And because it's dynamic, your IoT device inventory is always up to date. IoT Security also provides the automatic generation of policy recommendations to control IoT device traffic, as well as the automatic creation of IoT device attributes for use in firewall policies. Requires an IoT Security subscription.	**Minor Change –** IoT was not included in the v9.0 evaluation and should be excluded from the 10.0.5 evaluation also. The IoT security requires an IoT Security subscription which is not included in the evaluation. The ST and the AGD have been updated to exclude the IoT functionality.
Device-ID	The firewall can now collect metadata to detect and identify devices on your network and obtain recommendations on how to secure them so you can know what devices are connecting to your networks and use them as match criteria to create adaptive device-based policy rules. In environments with an increasing demand for "bring your own device" (BYOD) support and as more IoT (Internet of Things) devices connect to networks, detecting and securing these devices becomes increasingly difficult. By correlating network events with specific devices and providing actionable insights about them, Device-ID can quickly identify the source device for network incidents and help you create a responsive and comprehensive security policy.	**Minor Change –** The firewall can collect metadata to detect and identify devices on the network and obtain recommendations on how to secure them so you can know what devices are connecting to your networks and use them as match criteria to create adaptive device-based policy rules. The Device-ID functionality has not been tested in the evaluated configuration and is considered outside the scope of the evaluation.

Feature	Description	Rationale
		The ST and the AGD have been updated to exclude the Device-ID functionality.
Content Inspection Features Enhanced Pattern-Matching Engine for Custom Signatures	The PAN-OS® pattern-matching engine now supports new regular expression (regex) syntax and shorter data patterns, which dramatically expand the number of possible custom threat signatures that you can create and ingest from a third-party intrusion prevention system (IPS). To maximize the benefits of this new compatibility with third-party signatures, install the IPS Signature Converter for Panorama, which provides an automated solution for converting Snort and Suricata signatures into custom Palo Alto Networks threat signatures. You can also use the new pattern-matching capabilities to control application usage more finely with custom application signatures.	**Minor Change –** The following Panorama capabilities (i.e., stateful inspection filtering, IPsec VPN gateway, IPS/IDS threat prevention) are not evaluated (out of scope) in the previous evaluation. Only the secure communication channels from Panorama to firewalls and Wildfires are claimed. The functionality is not claimed in the v10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
IPS Signature Converter Plugin	The IPS signature converter plugin leverages the new Enhanced Pattern-Matching Engine to automatically convert rules for Snort and Suricata intrusion prevention system (IPS) software into custom Palo Alto Networks threat signatures. This enables you to immediately augment existing Threat Prevention coverage with Snort and Suricata rules that you receive from threat intelligence sources or that you write specifically for your network environment. Panorama 10.0 supports the IPS signature converter plugin and supplies the compatible version but does not install the plugin automatically. You should install the plugin if you have or expect to receive Snort and Suricata rules that you want to use in Security policy rules on your Panorama-managed firewalls.	**Minor Change –** The IPS signature converter plugin in an additional licensed product for the firewalls. The Panorama appliance is able to send Security policy rules to the Panorama-managed firewalls. However, the security target states that the Anti-Virus, Anti-Spyware, Anti-Malware security policies (i.e., profiles) are not evaluated and therefore, there features are out of scope. The security target states that only the secure communication (FPT_ITC.1) between the firewalls and the Panorama are claimed and validated in this evaluation. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
DNS Security Signature Categories	The DNS Security service now features individually configurable and extensible DNS Security Signature Categories, which enables you to create discrete Security policies based on the risk factors associated with certain types of DNS traffic. You can applying these new domain categories in your DNS Security policies to implement granular access control for different categories of domains based on the risk that these domains pose to your organization. These categories currently include C2 (encompasses DGA and DNS tunneling), malware, DDNS, newly registered domains, and phishing and we can expand these categories through PAN-OS content releases.	**Minor Change –** The WildFire appliance can be configured to locally generate antivirus and DNS signatures for discovered malware, and to assign a URL category to malicious links. The connected firewalls can be enabled to retrieve the latest signatures and URL categories every five minutes. However, the security target states that the File Blocking, DLP (Data Loss Prevention), and URL Filtering security policies/profiles are not evaluated and therefore, these features are out of scope. The security target states that only the secure communication (FPT_ITC.1) between the firewalls and the Wildfire are claimed and validated in this evaluation. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Expanded Data Collection for the DNS Security Service	The DNS Security service now collects additional server response and request information to provide improved analytics, DNS detection, and prevention.	**Minor Change –** The DNS Security service was not included in the v9.1.8 assurance maintenance and should not be included in the v10.0.5 evaluation. The change does not impact the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
URL Filtering Inline ML	The firewall can now use machine learning (ML) on the dataplane to analyze web page content and determine if the pages contain malicious JavaScript or other content used for credential phishing. Inline ML prevents web page threats from infiltrating your network by	**Minor Change –** The use of machine learning does not affect the claimed security functionality. This feature results in no changes to the ST or guidance

Feature	Description	Rationale
	providing real-time analysis capabilities on the firewall, which reduces the possibility of proliferation of unknown JavaScript variants and other phishing vectors.	documentation and has no effect on the result of any Assurance Activity test.
Increased Security Against Evasion Attacks	New protections bolster your defenses against evasion attacks where attackers attempt to breach your network by bypassing security inspection. The increased security measures cover evasion techniques that misuse URLs and Base64-encoded content. You begin receiving this protection as soon as you upgrade to a PAN-OS 10.0 release—no subscription or additional configuration is required.	**Minor Change –** The increased security measures cover evasion techniques that misuse URLs and Base64-encoded content does not affect the claimed security functionality.
NEW DECRYPTION FEATURE Decryption for TLSv1.3	You can now decrypt, gain full visibility into, and prevent known and unknown threats in TLSv1.3 protocol traffic. TLSv1.3 is the latest version of the TLS protocol, which provides security and performance improvements for applications. PAN-OS 10.0 supports TLSv1.3 decryption in all modes: SSL Forward Proxy, SSL Inbound Inspection, SSL Decryption Broker, and SSL Decryption Port Mirroring, and also for GlobalProtect Clientless VPN (browser to GlobalProtect Portal only).	**Minor Change –** TLS v1.3 is not claimed in the PP and should not be claimed in the maintenance assurance. The PAN-OS ST and Guidance has been updated to exclude this functionality.
Enhanced SSL Decryption Troubleshooting	You can now troubleshoot SSL Decryption-related issues and assess your security posture more easily with new Application Command Center (ACC) features and consolidated Decryption logs. Use the new ACC features to identify traffic for which decryption causes problems and then use the new Decryption logs to drill down into details and solve the problem. Also use the new ACC features to identify the amount of TLS traffic, non-TLS traffic, decrypted traffic, and non-decrypted TLS traffic. In addition, use the ACC to identify traffic that uses weak algorithms and protocols and mitigate the risk associated with applications, servers, and other devices that use older, more insecure protocols and algorithms.	**Minor Change –** Troubleshooting SSL Decryption-related issues is not a claimed security function in the ST and does not affect the security functionality. The previous security targets stated that the TLS and SSH decryption policies are not evaluated and therefore, these features are out of scope. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Block Export of Private Keys	You can now block the export of a private key when generating it on PAN-OS or Panorama, or when importing the key into PAN-OS or Panorama. Blocking key export hardens your security posture because it prevents rogue administrators from misusing keys. You can view which keys are blocked and which keys	**Minor Change –** Blocking the export of a private key when generating it on PAN-OS or Panorama, or when importing the key into PAN-OS or Panorama was not claimed in the previous evaluation and

Feature	Description	Rationale
	are not blocked. However, even an administrator with a Superuser role can't export blocked private keys.	should not be claimed in the Maintenance assures. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW MANAGEMENT FEATURE Web Interface Refresh	The PAN-OS® web interface has a new look and feel to provide an even better user experience. You can see the new branding, colors, and icons in Panorama™ and firewalls running a PAN-OS 10.0 release.	**Minor Change –** This new feature is not security related. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Telemetry	Telemetry data collection is expanded to cover device health and performance, product usage categories, and threat prevention. This data is used to power applications that increase your ability to manage and configure your Palo Alto Networks products and services and to provide improved visibility into device health, performance, capacity planning, and configuration. Palo Alto Networks uses this data to improve threat prevention and to help you maximize your product usage benefits.	**Minor Change –** This new feature is not security related. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
External Dynamic List Log Fields	The firewall now features new external dynamic list (EDL) log fields to help you quickly identify when an entry in an EDL matches traffic and to which EDL that entry belongs.	**Minor Change –** External Dynamic List Log Fields were not claimed in the previous evaluation and should not be claimed in the assurance maintenance. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Millisecond Granularity for PAN-OS® Logs	If you collect logs from multiple sources, you need detailed log timestamps for SOC troubleshooting, correlation, and visibility to investigate network security events and threats. Now all PAN-OS logs forwarded to an external destination, such as a syslog server or the Cortex™ Data Lake, support millisecond granularity timestamps.	**Minor Change –** The millisecond granularity of the timestamps does not affect the prior claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
PAN-OS and Panorama REST API Enhancements	The REST API now includes endpoints that enable you to manage network configurations on the firewall and on Panorama. Secondly, you can now configure administrative role types to provide granular access to REST API endpoints. You can enable, disable, or assign read-only access to each endpoint. Thirdly, access domain enforcement, which enables administrators to manage access to specific domains on Panorama and on firewalls, now extends to the REST API.	**Minor Change –** The enhancement of the REST API does not affect the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Proxy Support for Cortex Data Lake	You can now configure the firewall to forward logs to Cortex Data Lake through a proxy server. This enables you to send log data to Cortex Data Lake from a network without a default gateway.	**Minor Change –** The Cortex Data Lake was not included in the prior evaluation and should not be enabled in a maintenance assurance. The PAN-OS ST and Guidance has been updated to exclude this functionality.
Rule Usage Filtering Actions	Delete, disable, or tag policy rules directly from the Policy Optimizer after filtering unused rules to simplify your policy rule base management. For example, if you have a rule lifecycle process to identify obsolete rules, you can use the Policy Optimizer to filter, identify and tag the unused rules for offline review. After the review, you can return to view the list of tagged policy rules to delete any obsolete or unused rules.	**Minor Change –** The Policy Optimizer does not affect the claimed SFRs in the PAN-OS Security Target or the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Additional Predefined Time Filters for the ACC, Monitoring, and Reports	You can now filter the ACC, Monitoring, and Reports for up to 60 or 90 days. This enables improved performance when querying between 30 and 90 days by optimizing the Panorama query for only relevant logs.	**Minor Change –** The addition of Predefined Time Filters for the ACC, Monitoring, and Reports does not affect the claimed security functionality identified in the Security Target. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Enhanced Dataplane Processor Utilization Monitoring	You can now monitor individual dataplane (DP) processor utilization on firewalls with multiple dataplanes (PA-7000 and PA-5200 Series) using the Simple Network Management Protocol (SNMP) HOST-RESOURCES-MIB. Use the SNMP Manager to set alerts when utilization reaches	**Minor Change –** Monitoring individual dataplane (DP) processor utilization on firewalls with multiple dataplanes (PA-7000 and PA-5200 Series does not affect the

Feature	Description	Rationale
	a specific threshold for each DP processor to avoid service availability issues.	claimed security functionality in the PAN-OS Security Target. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Enhancements for Managing Update Server Connection	You now have improved visibility and troubleshooting for connections to the update server during firewall or Panorama management server registration, content updates, license renewals, and software upgrades. Enhancements include: System logs contain more specific reasons for communication issues such as command error, file I/O error, network failure, SSL verification failure, authentication failure, protocol error, and server error. You can configure up to three reconnection attempts if there is a connection failure. The default behavior (to not attempt to reconnect) is still the same. The content update package includes a SHA256 checksum of the package from the update server. You can validate this against checksum of the downloaded file to ensure the integrity of the downloaded content package.	**Minor Change –** Improved visibility and troubleshooting for connections to the update server during firewall or Panorama management server registration, content updates, license renewals, and software upgrades does not affect the prior claimed security functionality. Presently the TOE update is verified via a digital signature. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
New Regional Support for Telemetry (Supported in 10.0.2 and later)	For critical visibility into your deployment through telemetry-powered application and compliance with regional data privacy regulations, you can now send telemetry data to a storage destination in Canada, Japan, or Singapore. This feature requires Applications and Threats content version 8335 or later.	**Minor Change –** This feature was not included in the previous evaluation and does not affect the claimed security functionality in the ST. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW CERTIFICATE MANAGEMENT FEATURE Master Key Encryption Enhancement	On physical and virtual Palo Alto Networks appliances, you can now configure the Master Key to use the AES-256-GCM encryption algorithm to encrypt data. The AES-256-GCM encryption algorithm increases encryption strength to protect keys better and also includes a built-in integrity check. When you change the encryption level to AES-256-GCM, devices use it instead of the AES-256-CBC	**Minor Change –** Version 10.0.4 includes the option to use AES-GCM (256 bits) to encrypt the master key instead of AES-CBC (256 bits). By default, AES-CBC will be used to encrypt sensitive data. However, the admin can choose to switch to use the AES-GCM. This has no

Feature	Description	Rationale
	encryption algorithm when encrypting keys and other sensitive data.	impact as the administrator does not have to switch and even if they do, AES-GCM is still FIPS Approved and the Master key itself is still inaccessible to any unauthorized user. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
HSM Enhancements	Newer client driver versions are now supported for SafeNet and nCipher Hardware Security Module (HSM) appliances: SafeNet: You can select from versions 5.4.2 or 7.2. Additionally, you can choose to have your firewall authenticate and establish trust using manually generated certificates. nCipher nShield Connect: Version 12.40.2 is available (backward compatible up to v11.50 for older appliances)	**Minor Change –** The SafeNet and nCipher Hardware Security Module (HSM) appliances were not included in the previous evaluation and should not be used for a maintenance assurance. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW NETWORKING FEATURE IKEv2 Support for AES-GCM Encryption (Available with PAN-OS® 10.0.3 and later 10.0 releases)	Security-conscious customers in financial verticals and other markets who have VPN deployments are standardizing on strong IKE and IPsec security and require PAN-OS firewalls to support AES-GCM (Advanced Encryption Standard with Galois/Counter Mode). PAN-OS firewalls now support two new encryption algorithms for IKEv2 crypto profiles: AES-GCM with 128-bit strength and AES-GCM with 256-bit strength to provide compatibility with other devices and to provide stronger security than AES-CBC (AES with Cipher-Block Chaining).	**Minor Change –** All of the algorithms for IKE (and IPsec) are configurable. In the AGD guidance, Palo Alto specifies exactly which algorithms they can use. In this case, AES-GCM is not allowed for use in the CC evaluated configuration (at least not for IKE, it is allowed for IPsec though). This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Bonjour Reflector for Network Segmentation (Available with PAN-OS® 10.0.1 and later 10.0 releases)	To support Apple Bonjour in network environments that use segmentation to route traffic for security or administrative purposes (for example, where servers and clients are in different subnets), you can now forward Bonjour IPv4 traffic between Layer 3 (L3) Ethernet or Aggregated Ethernet (AE) interfaces or sub interfaces that you specify.	**Minor Change –** The Apple Bonjour in network environments for network segmentation was not claimed in the first evaluations and has not impact on the claimed security functionality.

Feature	Description	Rationale
	The Bonjour Reflector option allows you to forward multicast Bonjour advertisements and queries to up to 16 L3 Ethernet and AE interfaces or sub interfaces, ensuring user access to services and device discoverability regardless of Time To Live (TTL) values or hop limitations.	This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
HA Clustering for Multiple Data Centers	Data centers with multiple locations and high throughput need high availability (HA) with more than two members to ensure high reliability and to avoid a single point of failure. PAN-OS HA can now support clustering of up to 16 firewalls that perform session state synchronization. HA pairs in each data center prevent a single firewall failure and a data center failure, and asymmetric traffic from a data center is not dropped when sent to another data center.	**Minor Change –** High Availability was an optional configuration in the previous evaluation. High Availability does not impact the SFRs or claimed security functionality in the v10.0.5. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
HA Clustering for Horizontal Scaling of Firewalls	Within a data center, HA solutions must be able to scale horizontally. To provide seamless horizontal scalability of performance and capacity, PAN-OS HA can now support clustering of up to 16 firewalls that perform session state synchronization. In the event of a network outage or a firewall going down, the sessions fail over to a different firewall in the cluster.	**Minor Change –** High Availability was an optional configuration in the previous evaluation. High Availability does not impact the SFRs or claimed security functionality in the v10.0.5. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
HA Additional Path Monitoring Groups	To allow more flexible control over high availability (HA) deployments, you now have support for the use of multiple different destination IP groups within a single virtual wire (vwire), VLAN, and virtual router instance in PAN-OS and VMs. In addition to the option to set failure condition parameters for destination IP groups, you have greater granularity in controlling your HA failovers over those vwire, VLAN, and virtual router instances through segmentation.	**Minor Change –** High Availability was an optional configuration in the previous evaluation. High Availability does not impact the SFRs or claimed security functionality in the v10.0.5. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Packet Buffer Protection Based on Latency	Some protocols and applications are sensitive to latency; you can now enable packet buffer protection based on latency, which triggers protection before the latency affects the protocol or application. Packet buffer	**Minor Change –** The improvement of packet buffer protection does not affect the claimed security functionality in the 10.0.5 release.

Feature	Description	Rationale
	protection based on buffer utilization (which was available prior to PAN-OS 10.0) defends your firewall and network from single-session DoS attacks that can overwhelm the firewall's packet buffer and cause legitimate traffic to drop; it is now enabled by default.	This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Ethernet SGT Protection	In a Cisco TrustSec network, firewalls need to be able to identify and block packets that have specific Security Group Tags (SGTs) in their 802.1Q header. You can now do so at the ingress zone by creating a Zone Protection profile that lists SGTs to block, which results in better performance than blocking packets with security policy rules.	**Minor Change –** The SGT in a Cisco TrustSec network does not affect the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Aggregate Interface Group Capacity Increase	The need to support more link aggregation groups for network resiliency has increased as firewalls are positioned closer to endpoints to provide better visibility and control. The number of aggregate Ethernet (AE) interface groups that the PA-3200 Series, PA-5200 Series, and most PA-7000 Series firewalls support increased from 8 to 16. The exception is the PA-7000 Series firewall with PA-7000-100G-NPC-A and SMC-B, which increased from 8 to 32 AE interface groups. On all of these supported firewall models, QoS is supported on only the first eight AE interface groups.	**Minor Change –** The increase in the number of aggregate Ethernet (AE) interface groups does not affect the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
ECMP Strict Source Path	When you enable ECMP for a virtual router, IKE and IPsec traffic originating at the firewall by default egresses an interface that the ECMP load-balancing method determines. If the firewall has more than one ISP providing equal-cost paths to the same destination, one ISP could block legitimate traffic that arrives on an unexpected interface that ECMP chose. To avoid that problem, you can now enable ECMP Strict Source Path to ensure that IKE and IPsec traffic originating at the firewall always egresses the physical interface to which the source IP address of the IPsec tunnel belongs.	**Minor Change –** Equal Cost Multiple Path (ECMP) processing is a networking feature that enables the firewall to use up to four equal-cost routes to the same destination. The use of ECMP Strict Source Path does not have any impact on the claimed security functions. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Tunnel Acceleration for GRE, VXLAN, and GTP	Generic Routing Encapsulation (GRE), Virtual Extensible Local Area Network (VXLAN), and GPRS Tunneling Protocol (GTP) are now	**Minor Change –** GRE, GTP-U, and VXLAN tunnel acceleration do not have any impact on the

Feature	Description	Rationale
	supported by tunnel acceleration in the network processor, which improves performance and throughput. GRE and VXLAN tunnel acceleration—Supported on PA-3200 Series firewalls and PA-7000 Series firewall with a PA-7000-100G-NPC-A and a PA-7050-SMC-B or a PA-7080-SMC-B. GTP-U tunnel acceleration—Supported on PA-7000 Series firewalls with a PA-7000-100G-NPC-A and a PA-7050-SMC-B or a PA-7080-SMC-B.	claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW USER-ID FEATURE Streamlined and Resilient Redistribution	Redistribution for User-ID mappings is now more resilient, scalable, and easier to manage. The new data redistribution feature uses a more efficient distribution method, supports new filters for data types and network ranges, and provides a centralized interface and new CLI commands to troubleshoot and manage redistribution.	**Minor Change –** The User Identification Agent is installed on a separate dedicated PC in the operational environment to retrieve user-specific information that is uses for policy enforcement. The secure connection from the firewalls to the UIA is the only functionality covered in the evaluation. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Authentication with Custom Certificates for Redistribution	During redistribution, you can now use custom certificates issued by your enterprise certificate authority (CA) instead of predefined certificates to establish a unique chain of trust for mutual authentication between firewalls, between firewalls and User-ID agents, and between a firewall and Panorama.	**Minor Change –** The PAN-OS v9.1.8 ST states that The administrator may also import a certificate and private key into the TOE from an enterprise certificate authority or obtain a certificate from an external CA. This change does not have any impact on the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Enhanced Support for Syslog Messages	In dual-stacked environments where an endpoint has both an IPv4 and IPv6 address, the firewall can now match multiple IPv4 and IPv6 addresses in a single syslog message to	**Minor Change –** The enhanced support for syslog messages does not affect the claimed

Feature	Description	Rationale
	obtain IP address-to-username mappings. This eliminates the need to set up an infrastructure to send syslog messages through the firewall multiple times (due to multiple addresses per message). Additionally, the firewall can now parse syslog messages of up to 8,000 bytes to ensure the firewall successfully maps IP address-to-username information from User-ID sources that generate longer syslog messages.	security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW POLICY FEATURE IP Range and Subnet Support in Dynamic Address Groups	Dynamic address groups were previously limited to tagging single IP address for membership; only the first address in an IP group or subnet was included in the dynamic address group. You can now populate dynamic address group membership based on IP address ranges or IP subnets. This allows you to build and enforce policy based on changes in a specific range of IP addresses or on a particular subnet. For example, in a VMware NSX environment, if you run similar types of workloads on a dedicated IP range or subnet, it may not be efficient to tag every workload that joins the IP range. Now, you no longer need to tag each workload to ensure security. Additionally, you can see source and destination dynamic address groups in the firewall logs. This gives you additional visibility in your traffic logs for auditing and troubleshooting. And you can now take automated security actions on IP ranges and subnets, such as quarantining infected devices.	**Minor Change –** The IP Range and Subnet Support in Dynamic Address Groups does not affect the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
X-Forwarded-For HTTP Header Data Support in Policy	To help you enforce security policy on an endpoint that originates a request when it is behind an upstream device, such as an explicit HTTP proxy server or load balancer, the firewall can now use the source IP address contained in the X-Forwarded-For (XFF) field in the packet HTTP header. With the IP address of the original initiator of the request, you can ensure that the correct security policy rules are applied and use other features such as geo-blocking, IP blocking, and DoS protection. For example, if you want to block traffic originating in North Korea, so you create policy based on North Korean IP addresses. The firewall can identify those location-based IPs and enforce policy, even if that traffic passes through a explicit HTTP proxy. Additionally, the firewall now displays the endpoint IP address and	**Minor Change –** The use the source IP address contained in the X-Forwarded-For (XFF) field in the packet HTTP header affects the security policy rules but does not have any impact on the claimed security functional requirements in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
	upstream device IP address in logs to aid troubleshooting and remediation.	
NEW AUTHENTICATION FEATURE Authentication Portal Exclusion for Predefined Domains	Many applications require access to the internet for updates or other services, but in some cases, the Authentication policy may block access. To easily exclude benign background application traffic (such as Windows Update) on user devices from Authentication policy and prevent service interruption, you can use a new external dynamic list (EDL): the Palo Alto Networks Authentication Portal Exclude List. Palo Alto Networks maintains and updates this EDL so that you don't need to manually discover and add all the domains that background applications use to an allow list.	**Minor Change –** The Palo Alto Networks Authentication Portal Exclude List does not affect any of the claimed security functional requirements in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Improved Authentication Rate for Large-Scale Deployments	To enforce Authentication policy in environments with large numbers of users, the firewall now uses a multi-threaded process to simultaneously authenticate more users with protocols such as Security Assertion Markup Language (SAML), Kerberos, or the MFA API.	**Minor Change –** The protocols such as Security Assertion Markup Language (SAML), Kerberos, or the MFA API were not used in the first evaluation. The PAN-OS Security Target excludes external authentication servers and the use of SAML in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
TLS Encryption for Email Server Profiles	You can now configure the firewall and Panorama to send all data for an email server profile, including aggregated logs and reports, over an encrypted TLS connection (as long as the email server supports it). Using an encrypted TLS connection to securely send reports and logs prevents security risks, supports cloud-based email servers that require encryption, and helps ensure compliance with security audits.	**Minor Change –** Traffic logging and the use of email notifications and the SNMP and SMTP servers have not been subject to testing in the previous evaluation. As stated in the ST, they have not been subject to testing in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
NEW VIRTUALIZATION FEATURES Containerized Next-Generation Firewall for Securing Kubernetes Deployments	As you adopt Kubernetes and containers for application development and operational agility, you can now automate the deployment of the next-generation firewalls in environments such as OpenShift, native Kubernetes, GKE, AKS, or EKS, using native Kubernetes constructs. The CN-Series firewall is the containerized form factor of the next-generation firewall that provides complete Layer 7 visibility, application-level segmentation, and protection from advanced threats for traffic going between trust zones in public cloud or data center environments. The containerized form factor has a distributed PAN-OS architecture with CN-Mgmt and CN-NGFW pods that integrate into your CI/CD pipeline and help you secure traffic going from containerized applications running in Kubernetes clusters to VMs, bare metal servers, or to other containerized applications. The CN-Series firewall requires Panorama and the Kubernetes plugin on Panorama to enable centralized management, licensing, and security policy enforcement. Panorama and the CN-Series firewall use the Kubernetes APIs for a tight integration whereby the CN-NGFW pods that you deploy as a DaemonSet, use CNI-chaining for integrating into the container namespace and retrieve Kubernetes labels for enabling metadata-driven policies with dynamic address groups in Security policy.	**Minor Change –** The CN-Series firewall was not included in the first evaluation and are not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Automatic Site License Activation on the VM-Series Firewalls with Pay-As-You-Go (PAYG)	To support the automatic license activationworkflows for VM-Series use cases such as bootstrapping and autoscaling, the site licenses for AutoFocus and Cortex Data Lake can now be automatically activated for the Pay-as-you-go (PAYG) marketplace firewalls. With the support for enterprise wide (site) licenses on the VM-Series PAYG firewalls, these firewalls can now access the cloud-based threat intelligence service (AutoFocus) and logging infrastructure (Cortex Data Lake) within your enterprise. When you provide the auto-registration pin ID and value as part of the bootstrapping process, the firewall is automatically registered to the Customer Support Account so that it can retrieve the site licenses that have already been registered on the Customer Support Portal. You can also	**Minor Change –** Site Licenses do not have any impact on the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
	manually retrieve the license directly on the firewall.	
vMotion Support for the VM-Series Firewall on VMware ESXi and VMware NSX-T (Available with PAN-OS 10.0.1 and later releases)	You can now use VMware's vMotion functionality to move the VM-Series firewall deployed in ESXi or NSX-T without impacting active traffic sessions.	**Minor Change –** The use VMware's vMotion functionality to move the VM-Series firewall deployed in ESXi or NSX-T without impacting active traffic sessions does not affect the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Traffic Inspection for Pods with Multiple Network Interfaces using Multus CNI (Available with PAN-OS 10.0.1 and later releases)	In OpenShift deployments where application pods have multiple interfaces, you can configure the CN Series firewall to inspect traffic from all the interfaces or a selected number of interfaces. To secure traffic going through secondary interfaces on a multi-homed pod, the Multus container networking interface (CNI) is required with a bridge-based connection to the additional networks.	**Minor Change –** The CN-Series firewall was not included in the first evaluation and are not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
5G-Native Security on CN-Series (Available with PAN-OS 10.0.3 and later releases)	To secure the highly distributed 5G networks, including edge clouds and across multi-vendor and multi-cloud environments, you can enable network slice security, equipment ID security, and subscriber ID security on the CN-Series. Security policy rules and correlation based on 5G network slice, equipment ID, and subscriber ID are supported. You can also enable RAN-based security with SCTP and GTP Security for 5G user-plane tunnel content inspection and threat prevention. The CN-Series firewall is supported on VMWare's VMware Tanzu Kubernetes Grid (TKG) platform with the Intel x710, macvlan and Multus CNI's available as part of TKG - SR-IOV.	**Minor Change** – The CN-Series firewall was not included in the first evaluation and are not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW SD-WAN FEATURES Full Mesh VPN Cluster with DDNS Service	If you place your SD-WAN branch firewall behind a device performing NAT, you need a way to specify the IP address of the public-facing interface on that upstream device, which Auto VPN Configuration uses as the tunnel endpoint for the branch. When you add	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin.

Feature	Description	Rationale
(Available with PAN-OS® 10.0.3 and later 10.0 releases)	an SD-WAN branch to Panorama, you can now specify the IP address or FQDN of the upstream device performing NAT for the branch, or you can specify DDNS, which indicates that the IP address for the interface on the NAT device is obtained from the Palo Alto Networks DDNS service. Auto VPN uses the public IP address as the tunnel endpoint for the branch.	The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
Auto-VPN Configuration with Branch Behind NAT (Available with PAN-OS 10.0.3 and later 10.0 releases)	If you place your SD-WAN branch firewall behind a device performing NAT, you need a way to specify the IP address of the public-facing interface on that upstream device, which Auto VPN Configuration uses as the tunnel endpoint for the branch. When you add an SD-WAN branch to Panorama, you can now specify the IP address or FQDN of the upstream device performing NAT for the branch, or you can specify DDNS, which indicates that the IP address for the interface on the NAT device is obtained from the Palo Alto Networks DDNS service. Auto VPN uses the public IP address as the tunnel endpoint for the branch.	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin. The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
DIA AnyPath (Available with PAN-OS 10.0.3 and later 10.0 releases)	You can now configure an SD-WAN direct internet access (DIA) link to fail over to another link that has a direct or indirect path (through a hub or branch) to the internet, and thus ensure business continuity. The DIA failover is no longer restricted to another DIA link. DIA AnyPath use cases include transitioning from an expensive MPLS link to one or more public internet connections, possibly from different vendors. You can do split tunneling per application, where specific applications initially use a DIA link but fail over to a hub link, or vice versa.	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin. The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
SD-WAN Forward Error Correction (Available with PAN-OS® 10.0.2 and later 10.0 releases)	When both endpoints of a VPN tunnel are PAN-OS firewalls that use forward error correction (FEC), the receiving tunnel endpoint can recover lost packets before the link needs to fail over to a better path. Thus, FEC at the network level allows you to maintain a high-quality application experience in your SD-WAN. FEC is especially helpful for applications that are sensitive to packet loss, such as voice and video streaming.	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin. The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
SD-WAN Packet Duplication (Available with PAN-OS® 10.0.2	PAN-OS 10.0.2 now allows SD-WAN to accurately monitor and measure the health of SaaS and Cloud application path to ensure reliability and user experience. When you have	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin.

Feature	Description	Rationale
and later 10.0 releases)	an SD-WAN firewall with Direct Internet Access (DIA) link, SD-WAN fails over to a higher performance path based on accurate measurements of the path health quality. SD-WAN visibility and monitoring now reflect the SaaS measurements for latency, jitter, and packet loss for Direct Internet Access (DIA) links.	The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
SaaS Application Path Monitoring (Available with PAN-OS 10.0.2 and later 10.0 releases)	PAN-OS 10.0.2 now allows SD-WAN to accurately monitor and measure the health of SaaS and Cloud application path to ensure reliability and user experience. When you have an SD-WAN firewall with Direct Internet Access (DIA) link, SD-WAN fails over to a higher performance path based on accurate measurements of the path health quality. SD-WAN visibility and monitoring now reflect the SaaS measurements for latency, jitter, and packet loss for Direct Internet Access (DIA) links.	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin. The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
Application and Link Performance Monitoring (Available with PAN-OS 10.0.2 and later 10.0 releases)	SD-WAN monitoring and visibility now allow you to better understand the effectiveness of Forward Error Correction (FEC) and packet duplication for paths with degraded health metrics.	**Minor Change -** The PAN-OS 9.1.8 Firewall evaluation did not include the SD-WAN plugin. The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
NEW MOBILE INFRASTRUCTURE SECURITY FEATURES Session persistence during rate limiting for GTP and SCTP brute force attack signatures (Available with PAN-OS® 10.0.2 and later 10.0 releases)	To provide more intelligent and flexible traffic control while protecting against flooding attacks for GTP or SCTP (including Diameter-S6a and S1AP) messages, the firewall now keeps existing sessions open if the number of SCTP or GTP packets exceeds the specified threshold and the Action for the brute force signature is drop. If the number of SCTP packets exceeds the threshold, the firewall nullifies the data chunks that match the context in the child signature for the remaining duration of the threshold. If the number of GTP packets exceeds the threshold, the firewall drops the packets that match the context in the child signature but the session remains open, which allows other GTP traffic for the remainder of the specified interval.	**Minor Change -** Session persistence during rate limiting for GTP and SCTP brute force attack signatures does not have any impact on the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
Network Slice Security in a 5G Network	Network operators lack tools to investigate security events related to enterprises and industry verticals served by network slices in 5G. Also, they are unable to offer customizable, advanced network security capabilities that can be dynamically created per network slice. You can now apply context-aware network security to an enterprise or customer from a vertical industry that is using a 5G network by creating Security policy rules based on network Slice/Service Type (SST). The firewall supports standardized SSTs and operator-specific SSTs.	**Minor Change -** The use of 5G networks were not identified in the evaluated configuration of the previous evaluation and is not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Equipment ID Security in a 5G Network	In 5G, HTTP/2 replaces the GTP-C and Diameter protocols; therefore, existing network security technologies relying on GTP-C and Diameter protocols for extracting context, such as equipment ID or International Mobile Equipment Identity (IMEI), will not work in 5G. Network operators lack tools in 5G to investigate security events related to equipment and devices. Because the majority of IP addresses assigned to equipment and devices connected to 5G networks are dynamic, context-aware security capability based on Equipment ID is required to secure them and protect the network from compromised or disallowed equipment and devices. You can now apply Security policy rules based on the equipment identity (Permanent Equipment Identifier [PEI] including IMEI) of a device, such as an IoT device, phone, or tablet, in your 5G network.	**Minor Change -** The use of 5G networks were not identified in the evaluated configuration of the previous evaluation and is not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Subscriber ID Security in a 5G Network	In 5G, HTTP/2 replaces the GTP-C and Diameter protocols; therefore, existing network security technologies relying on GTP-C and Diameter protocols for extracting context, such as subscriber ID or International Mobile Subscriber Identity (IMSI), will not work in 5G. Network operators lack tools in 5G to investigate security events related to subscribers and users. Because the majority of IP addresses assigned to subscribers and users connected to 5G networks are dynamic, context-aware security capability is required to secure them and protect the network from compromised or disallowed subscribers and users. You can now apply Security policy rules based on the subscriber ID (Subscription	**Minor Change -** The use of 5G networks were not identified in the evaluated configuration of the previous evaluation and is not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
	Permanent Identifier [SUPI] including IMSI) of a subscriber or user in your 5G network.	
Equipment ID Security in a 4G Network	Because the majority of IP addresses assigned to equipment and devices connected to 4G/LTE networks are dynamic, context-aware security capability based on equipment identity is required to secure them and protect the network from compromised or disallowed equipment and devices. You can now apply Security policy rules based on the International Mobile Equipment Identity (IMEI) of a device, such as an IoT device, phone, or tablet, in your 4G/LTE network.	**Minor Change** - The use of 4G networks were not identified in the evaluated configuration of the previous evaluation and is not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Subscriber ID Security in a 4G Network	Because the majority of IP addresses assigned to subscribers and users connected to 4G/LTE networks are dynamic, context-aware security capability based on subscriber identity is required to secure them and protect the network from compromised or disallowed subscribers and users. You can now apply Security policy rules based on the International Mobile Subscriber Identity (IMSI) of a subscriber or user in your 4G/LTE network.	**Minor Change -** The use of 4G networks were not identified in the evaluated configuration of the previous evaluation and is not included in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
NEW HARDWARE PA-7000 Series Data Processing Card (DPC)	Improve the performance of more resource-heavy security features, such as Threat Prevention and SSL Decryption, by installing the PA-7000-DPC-A. The DPC (data processing card) is a new computing card for the PA-7000 Series firewalls compatible with all prior NPCs. Each DPC adds four additional instances of the PAN-OS data plane, providing 133% of the computing capacity compared to the three data planes on the PA-7000-100G-NPC-A.	**Minor Change –** The PA-7000 Series Data Processing Card (PA-7000-DPC-A) is an optional interface card that can be installed to improve the performance and processing capacity of the PA-7000 chassis. Similar in physical design to the PA-7000 100G NPC, the DPC offers scalability in the form of four additional data plane instances. As opposed to the PA-7000 100G NPC, the DPC does not have a network processor or a physical I/O (e.g., no ethernet port); therefore, the firewall must have at least one or more PA-7000 Series Firewall Network Processing Cards (NPCs). The PA-7000-DPC-A card was tested as part of the regression testing (which includes the PA-7000 chassis)

Feature	Description	Rationale
		to verify functionality. In addition, performance testing was done to demonstrate its session load balance capability. The DPC introduces no new security functionality claimed in the ST.
PA-3200 Series HA-1 Port Remapping for PAN-OS and Panorama	You now have the choice to map your PA-3200 Series firewall's copper HA-1 port to one of the firewall's available fiber SFP ports. The fiber port enables longer distance HA connectivity for use in data centers and provides the same HA-1 port functionality.	**Minor Change -** The addition of the PA-3200 Series firewall's copper HA-1 port to one of the firewall's available fiber SFP ports does not affect the claimed security functionality in the 10.0.5 release. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
1G Transceiver Support on PA-7000-20GQ-NPC and PA-20GQXM-NPC Cards	PAN-OS can now recognize 1G SFP transceivers in PA-7000 Series firewall PA-7000-20GQ-NPC and PA-20GQXM-NPC cards. With this feature, you have more control over SFP connectivity and a choice between a rate of 1G or 10G.	**Minor Change -** The SFP input/output transceivers do not have any impact on the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
PA-7000-100G-NPC-A Breakout Cable Support	You now have support for the use of SR4 transceivers (PAN-QSFP-40GBASE-SR4 or PAN-QSFP28-100GBASE-SR4) that allow a PA-7000 Series firewall's QSFP/QSFP+ ports to be configured as four interfaces. When broken out with an appropriate breakout-cable the individual QSFP physical interfaces are able to provide four separate 10G or 25G interfaces.	**Minor Change -** The SFP input/output transceivers do not have any impact on the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
PA-7000-LFC-A Breakout Cable Support	You now have support for link aggregation on the PA-7000 Series LFC-A cards. With link aggregation, you can breakout the LFC-A's QSFP+ connection into up to four 10G links in conjunction with the PAN-QSFP-40GBASE-SR4 transceiver and appropriate breakout-cable, providing physical layer redundancy for the firewall's outgoing connection.	**Minor Change -** The breakout cable support does not have any impact on the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
Changes to Default Behavior Multiple APNs on S11 interfaces for RAN deployments	In PAN-OS 10.0.2 and earlier, all access point names (APNs) from the same user equipment (UE) shared a single GTP-C tunnel on an S11 interface. In PAN-OS 10.0.3 and later, the firewall supports multiple APNs on an S11 interface for RAN deployments by creating separate sessions for multiple APNs. By dividing the GTP-C tunnel into multiple sessions, the firewall now processes each APN independently.	**Minor Change –** Multiple access point names being divided into multiple sessions to process independently does not affect the claimed security functionality or the SFRs in the 10.0.5 release.
Session persistence during rate limiting for GTP and SCTP brute force attack signatures	In PAN-OS 9.1 and earlier, if the number of packets matching the context of the brute force signature for GTP and SCTP (including Diameter-S6a and S1AP) per-message signatures exceeded the threshold and the Action was drop, the firewall would deny any further traffic for the session and drop any subsequent packets. In PAN-OS 10.0.2 and later, the firewall keeps the session open and drops packets on a per-session basis only if they match the brute force signature. For example, if the rate limit configuration is five packets every two seconds, the firewall allows the first four packets; the fifth and any subsequent packets are dropped for the two-second threshold duration.	**Minor Change –** Session persistence during rate limiting for GTP and SCTP brute force attack signatures does not have any impact on the claimed security functionality.
Packet Buffer Protection	On all firewall models, packet buffer protection based on packet buffer utilization percentage is enabled by default globally and on each zone.	**Minor Change –** The improvement of packet buffer protection does not affect the claimed security functionality.
VM-Series Disk Upgrade Restriction	In PAN-OS version 9.0 and higher the recommended minimum disk size for VM-Series firewalls was 60GB, but PAN-OS did not prevent the upgrade if the minimum was not met. PAN-OS version 10.0 disallows upgrade if your VM-Series firewall disk size is less than 60GB.	**Minor Change –** The size of the VM disk does not affect the claimed security functionality in the ST or the 10.0.5 release.
Access Domain for REST API	Access domains enable administrators to manage access to specific domains on Panorama and on firewalls with multiple virtual systems. Access domain enforcement now extends to the REST API.	**Minor Change –** The enhancement of the REST API does not affect the claimed security functionality in the ST or the 10.0.5 release.
PAN-OS and Panorama REST API Enhancements	After you upgrade to PAN-OS version 10.0, the initial REST API access privileges for admin role profiles will default to Disabled. If you downgrade from PAN-OS version 10.0 to 9.1,	**Minor Change –** The enhancement of the REST API does not affect the claimed

Feature	Description	Rationale
	the admin role profiles will preserve the XML API access privileges, and the preserved XML API access privileges will determine the REST API access privileges.	security functionality in the ST or the 10.0.5 release.
Authentication policy	Previously, the firewall required traffic decryption before enforcing Authentication policy. Now, the firewall enforces Authentication policy for all encrypted TLS traffic without requiring decryption. To ensure that this change in behavior doesn't block users from resources they could access prior to this change, we recommend making the following changes: Decrypt all web traffic that matches your Authentication policy so that users must authenticate using Captive Portal. Enable GlobalProtect clients to receive notifications to complete the authentication process. If you do not use GlobalProtect and you do not want to decrypt all web traffic, modify your Authentication policy so that it excludes encrypted traffic. Configure an Authentication Portal Exclude List to exclude background traffic from authentication for approved applications.	**Minor Change –** The previous PAN-OS evaluation verified only the secure communication channel between the Firewall and the GlobalProtect. The enhancement does not affect the claimed security functionality in the ST or the 10.0.5 release.
NT LAN Manager protocol	Due to the inherent security risks of this legacy protocol, the NT LAN Manager (NTLM) authentication protocol has been removed in this release. We recommend using Kerberos Single Sign-On (SSO) or Security Assertion Markup Language (SAML) for SSO authentication.	**Minor Change** - The use of NT LAN was not identified in the previous evaluation and does not have any effect on the claimed SFRs.
User-ID Redistribution for Dedicated Log Collectors	The Dedicated Log Collector no longer supports redistribution for User-ID information in this release. We recommend using the firewall or Panorama to redistribute information.	**Minor Change –** The User Identification Agent is installed on a separate dedicated PC in the operational environment to retrieve user-specific information that is uses for policy enforcement. The secure connection from the firewalls to the UIA is the only functionality covered in the evaluation. This feature results in no changes to the ST or guidance documentation and has no

Feature	Description	Rationale
		effect on the result of any Assurance Activity test.
Collector Groups	The minimum number of Log Collectors required for a Collector Group to be operational is based on the following formula where n equals the total number of Log Collectors in the Collector Group: n/2+1 For example, if you configure a Collector Group with six Log Collectors, a minimum of four Log Collectors are required for the Collector Group to be operational.	The minimum number of Log Collectors required for a Collector Group to be operational does not impact any of the claimed security functionality.
SSL Decryption profile TLS maximum version	In PAN-OS 9.1 and earlier, the default Max Version in the SSL Decryption profile's SSL Protocol Settings was Max so that profiles automatically used the newest TLS version without manual reconfiguration. In PAN-OS 10.0, the default Max Version changed to TLSv1.2 to prevent any service disruption of mobile applications that enforce certificate pinning.	**Minor Change -** The TLS decryption policies are not evaluated and therefore, these features are out of scope.
Context Switch	After you upgrade to PAN-OS 10.0, you must assign a Device Admin Role that is pushed to your managed firewalls when configuring a Panorama Admin Role profile to allow Device Group and Template administrators to context switch between the Panorama and firewall web interface.	**Minor Change -** The Device Administrator was previously identified in the PAN-OS 9.1.8 ST. All administrators are identified as the Security Administrator as defined in the NDcPP. This does not have an impact on the assurance maintenance.
Device-ID	In PAN-OS 9.1 and earlier, the firewall used the Palo Alto Networks Services service route to send Enhanced Application Logs (EAL logs). In PAN-OS 10.0 and later versions, the firewall sends EAL logs using the Data Services service route, which uses the management interface by default. Other services, such as Data Loss Prevention (DLP), also use this service route. You can configure any Layer 3 (L3) interface, including the management or dataplane interfaces, for the service route. If your firewall currently sends EAL logs (for example, if you are using Cortex XDR), the firewall automatically uses the Data Services service route after you upgrade to PAN-OS 10.0. If you want to use a different interface	**Minor Change -** The PAN-OS v9.1.8 ST states that the standalone TOE stores the audit records locally. This change in the default behavior does not affect the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Feature	Description	Rationale
	for the service route, you can change the service route to any L3 interface. If you use a log forwarding card (LFC) with the 7000 series, when you upgrade to PAN-OS 10.0, you must configure the management plane or dataplane interface for the service route because the LFC ports do not support the requirements for the service route. We recommend using the dataplane interface for the Data Services service route.	
Log Forwarding	The PA-7000 series firewall utilizing a Log Forward Card does not forward logs to an M-Series appliance in Panorama or Log Collector mode with 10GB network interfaces. To successfully forward logs from a PA-7000 series firewall utilizing a Log Forwarding Card, a network switch must be present between the PA-7000 series lfp0 or lfp1 interfaces of the Log Forwarding Card and the M-Series appliance for the PA-7000 series firewall.	**Minor Change -** The Log Forward Card was not claimed in the previous evaluation and is not claimed in the maintenance assurance.
Terminal Server (TS) agent	Previously, to exclude the IP Address and Alternative IP Addresses of a Terminal Server (TS) Agent host from IP address-to-user mappings, you needed to manually enter those IP Addresses in the Exclude list. Now, the firewall automatically excludes these IP Addresses from IP address-to-user mapping.	**Minor Change -** The Terminal Server (TS) Agent was not claimed in the previous evaluation and is not included in the 10.0.5 release.
User-ID	Previously, if User-ID could not identify a user from the existing mappings, it would send a query for updated user mappings to all User-ID agents, which was useful if there was a longer time interval between updates. Now, the agents send the mapping updates to the firewall or Panorama in real time so there is no need to send the query for new mappings.	**Minor Change –** The User Identification Agent is installed on a separate dedicated PC in the operational environment to retrieve user-specific information that is uses for policy enforcement. The secure connection from the firewalls to the UIA is the only functionality covered in the evaluation. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Captive Portal (Authentication Portal)	To improve security, the firewall now generates a token parameter for the Authentication Portal URL when the user's web traffic matches an Authentication Policy rule. If you have shared or bookmarked a URL for the	**Minor Change -** The new default behavior does not affect the claimed security functionality in the security target.

Feature	Description	Rationale
	Authentication Portal page, after you upgrade to PAN-OS 10.0, update the bookmarked URL by removing the URL parameter or disable the token generation using the following CLI command in Configure mode: set deviceconfig setting captive-portal disable-token yes, then commit the changes using the commit command.	
Local Administrator Authentication	If you have a local administrator account that authenticates using a remote authentication server such as a SAML Identity Provider (IdP), you must ensure that the username that the authentication server sends to the firewall or Panorama doesn't contain a domain and is identical to the username in the local administrator account settings on the firewall or Panorama.	**Minor Change -** The previous evaluation did not include a remote authentication server such as SAML and as such should not be used in the maintenance assurance. The ST and AGD have been updated to exclude the SAML Identity Provider (IdP).
SAML Authentication	The *None* option for the Identity Provider Certificate in the SAML Identity Provider server profile has been removed in this release. To ensure the integrity of the SAML Responses or Assertions from Identity Provider (IdP), the firewall or Panorama requires an IdP certificate. The firewall or Panorama always validates the signature of the SAML Responses or Assertions against the IdP certificate that you configure.	**Minor Change -** The previous evaluation did not include a remote authentication server such as SAML and as such should not be used in the maintenance assurance. The ST and AGD have been updated to exclude the SAML Identity Provider (IdP).
PA-7000 Series Firewall Memory Limit for the Management Server	As of PAN-OS 10.0.1, the PA-7000 Series firewalls have new CLI commands to enable or disable resource control groups and new CLI commands to set an upper memory limit of 8G on a process (mgmtsrvr). To enable resource-control groups, use: • debug software resource-control enable To disable resource-control groups, use: • debug software resource-control disable To set the memory limit, use: • debug management-server limit-memory enable To remove the memory limit, use: • debug management-server limit-memory disable • Reboot the firewall to ensure the memory limit change takes effect.	**Minor Change -** The memory limit on a firewall does not affect the claimed security functionality. This feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Device Administrator	Non-superuser administrators with all rights enabled can Review Policies or Review Apps for downloaded or installed content versions.	**Minor Change -** The Device Administrator role is identified as the security administrator as

Feature	Description	Rationale
		defined in the NDcPP. No claimed security functionality in the ST has been changed.
SSH Service Profile	In PAN-OS 9.1 and earlier releases, you could generate a new pair of public and private SSH host keys and change other SSH configuration parameters such as the default host key type from the CLI. In PAN-OS 10.0 and later releases, you must create an SSH service profile (DeviceCertificate Management SSH Service Profile) to customize management and HA SSH configurations. You can configure these profiles from the CLI or the firewall or Panorama web interface.	**Minor Change -** The SSH service profile does not affect the basic operation of SSH. The claimed security functionality in the ST has not been modified.

Equivalency Discussion

No functionality, as defined in the SFRs, was impacted by the Palo Alto PAN-OS v10.0.5 software update of the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewalls.

The functionality of the PAN-OS v10.0.5 software update remains the same as prior evaluated version.

Product Changes

For this Assurance Continuity, the change consists of making the following firmware minor version updates and the removal of the PA-3000 Series Firewalls.

- From: Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0
- To: Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0

The PA-3000 Series (PA-3020, PA-3050, PA-3060) Firewalls have reached End-of-Life and are no longer considered part of the evaluated configuration.

The following are new features or product improvements added to PAN-OS since the previous Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8 evaluation.

The addition of the optional Palo Alto PA-7000-DPC-A Network Processing Card is considered equivalent to the other five Network Processing Cards. The same networking functionality is performed. The only difference is the speed and bandwidth of the card.

The following new feature additions do not change the security functionality of the TOE. The ST and the AGD documents have been updated to exclude the functionality from the assurance maintenance.

Feature	Description
SD-WAN	The PAN-OS software can include a native SD-WAN subscription to provide intelligent and dynamic path selection on top of what the

	PAN-OS security software already delivers. Secure SD-WAN provides the optimal end user experience by leveraging multiple ISP links to ensure application performance and scale capacity. The SD-WAN capability is considered out of scope. The ST and Guidance have been updated to exclude the SD-WAN plugin from the 10.0.5 evaluation.
Include Username in HTTP Header Insertion Entries	Allows the firewall to relay a user's identity when they are accessing your network through secondary security appliances that are connected to your Palo Alto Networks firewall. You can configure your firewall to include the username in the HTTP header so that other security appliances in your network can identify the user without additional infrastructure (such as proxies used to insert the username). This simplifies deployment, reduces page-load latency, and eliminates multiple authentications for users. This feature is outside the scope of the evaluation. The ST and AGD have been updated to exclude the Include Username in HTTP Header Insertion Entries from the evaluation.
SAML Authentication	SAML Authentication is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP). External authentication is outside the scope of the evaluation. The ST and AGD have been updated to exclude the SAML Identity Provider (IdP).
IoT Security	The IoT Security solution works with next-generation firewalls to dynamically discover and maintain a real-time inventory of the IoT devices on your network. Through AI and machine-learning algorithms, the IoT Security solution achieves a high level of accuracy, even classifying IoT device types encountered for the first time. And because it's dynamic, your IoT device inventory is always up to date. IoT Security also provides the automatic generation of policy recommendations to control IoT device traffic, as well as the automatic creation of IoT device attributes for use in firewall policies. Requires an IoT Security subscription. IOT Security is outside the scope of the evaluation. The ST and AGD have been updated to exclude the IoT Security.
Device-ID	The firewall can collect metadata to detect and identify devices on the network and obtain recommendations on how to secure them so you can know what devices are connecting to your networks and use them as match criteria to create adaptive device-based policy rules. The Device-ID functionality has not been tested in the evaluated configuration and is considered outside the scope of the evaluation. The ST and AGD have been updated to exclude the Device-ID functionality.
TLS v1.3	TLSv1.3 is the latest version of the TLS protocol, which provides security and performance improvements for applications. TLSv1.3 is outside the scope of the evaluation. The ST and AGD have been updated to exclude TLS v1.3.
Proxy Support for	The firewall can be configured to forward logs to Cortex Data Lake

Cortex Data Lake	through a proxy server. This enables you to send log data to Cortex Data Lake from a network without a default gateway. The forwarding of logs to Cortex Data Lake is outside the scope of the evaluation. The ST and AGD have been updated to exclude the Proxy Support for Cortex Data Lake.

Changes to the Development Environment

Palo Alto updated the ST to identify the maintained TOE. The ST for the maintained TOE is:

- Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0 Security Target, Version 1.0 June 1, 2021

Affected Developer Evidence

This section identifies all of the CC evidence previously subject to evaluation along with a summary of how each has been affected by the product updates for the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0.

(Note that the evidence identified in the left column identifies the original versions; and the second column identifies the changes in this maintenance)

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8 Security Target, Version 1.3, April 22, 2021	**Maintained Security Target:** Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0 Security Target. Version 1.0, June 1, 2021 Changes in the maintained ST are: • Updated identification of ST • Section 1.1 - Updated TOE software version • Section 1.1 – Deleted the PA-3000 Series Firewalls • Footnote 1 – Added the additional 7000-DPC-A Network Processing Card • Section 2.1 - Updated the PAN-OS version number and deleted the PA-3000 Series Firewalls • Section 2.2.1 - Updated the PAN-OS version number and deleted the PA-3000 Series Firewalls • Table 1 – Deleted the PA-3000 Series Firewalls • Section 2.3 – Identified the most current documentation for the current PAN-OS release 10.0.5 • Section 2.4 Updated the evaluation excluded features for the new release 10.0.5 product improvements or features.

Evidence Identification	Effect on Evidence/ Description of Changes
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS 9.1.8, March 15, 2021	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS 10.0, June 1, 2021 Changes in the maintained Guidance are: • Updated Section *Scope of Evaluation* - Updated the list of protocols or features that are not evaluated and considered out of scope. • Section 1.2 *TOE References* – Deleted the PA-3000 Series Firewalls. Updated the version to 10.0.5 • Section 1.3 Documentation References – Updated and identified the current documentation set for the 10.0.5 release. • Section 6 Evaluated Configuration – Updated for new commands and GUI screenshots.

Assurance Continuity Maintenance Report

- Leidos submitted an Impact Analysis Report (IAR) on behalf of Palo Alto for the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0 since the previous Common Criteria evaluation (CCEVS-VR-VID11063-2020).
- The PA-3000 Series (PA-3020, PA-3050, PA-3060) Firewalls have reached End-of-Life and are no longer considered part of the evaluated configuration.
- The Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall was updated from version PAN-OS 9.1.8 to version PAN-OS 10.0.5. The software updates included new non-security relevant features and bug fixes. The software updates and their effects and relevance are summarized below.
- Support for the optional Palo Alto PA-7000-DPC-A Network Processing Card has been added to the evaluation.

Regression Testing

Palo Alto Networks has completed extensive regression testing on PAN-OS version 10.0. The regression testing was performed on all maintenance versions (i.e., 10.0.4, 10.0.5) and on all the platforms including the PA-7000 and virtual VM-Series. There are two types of tests: Automated and Manual. The automated regression test runs consist of 6,774 tests run across different features on 10.0.x to verify all old and new features. The test runs verified that all new features work as expected, and previous features as well (i.e., ensure new features do not break old features). Any test case failures were tracked, and all the bugs found were fixed and verified. For manual testing, QA engineers have executed over 548 test cases across all platforms on 10.0.0 base image and also some bug verification and retest across different 10.0.x releases.

The PA-7000 Series Data Processing Card (PA-7000-DPC-A) is an optional interface card that can be installed to improve the performance and processing capacity of the PA-7000 chassis. Similar in physical design to the PA-7000 100G NPC, the DPC offers scalability in the form of four additional data plane instances. As opposed to the PA-7000 100G NPC, the DPC does not have a network

processor or a physical I/O (e.g., no ethernet port); therefore, the firewall must have at least one or more PA-7000 Series Firewall Network Processing Cards (NPCs). The PA-7000-DPC-A card was tested as part of the regression testing (which includes the PA-7000 chassis) to verify functionality. In addition, performance testing was done to demonstrate its session load balance capability. The DPC introduces no new security function.

Finally, the evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. The search did not identify any new potential vulnerability.

Vulnerability Assessment

A public search for new vulnerabilities that might affect the TOE since the evaluation was completed was performed. In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version update.

The vulnerability searches were performed on the Palo Alto products that are posted on the NIAP Product Compliant List web pages that implement PAN-OS. PAN-OS is integral to the following Palo Alto products.

CCEVS-VR-VID11063-2020 - Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0. Certificate Date: 2020.10.14
The original search terms for the evaluation listed above have been provided below. All searches below were performed on 6/1/2021 and go back to the date of 4/22/2021 to the prior assurance maintenance.

Databases used for the searches:

- http://web.nvd.nist.gov/view/vuln/search
- https://securityadvisories.paloaltonetworks.com

Search terms

- Linux 3.10 (TOE implements Linux 3.10.88)
- Microarchitectural
- Palo Alto
- N/A - https://securityadvisories.paloaltonetworks.com
- VM-Series
- PAN-OS
- Router
- Switch
- Firewall
- TCP
- UDP
- IPv4
- IPv6
- SSH
- HTTPS
- TLS
- IPsec
- Cavium

Search Term: = Linux 3.10

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "Linux 3.10" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A			

Search Term: = Microarchitectural

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "Microarchitectural" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A			

Search Term: = Palo Alto

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "Palo Alto" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A			

Search Term: = TCP

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "TCP" identified two new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A	The resulting vulnerability search identified two new vulnerabilities since the prior 4/22/2021 assurance maintenance search. Neither vulnerability was related to the TOE nor were they related to TCP vulnerabilities in general.	N/A	The TOE is not vulnerable.

Search Term: = SSH

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "SSH" identified nine new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A	The resulting vulnerability search identified two new vulnerabilities since the prior 4/22/2021 assurance maintenance search. None of the vulnerabilities were related to the TOE nor were the respective entries involving SSH did not appear to be relevant to the TOE.	N/A	The TOE is not vulnerable.

Search Term: = HTTPS

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "HTTPS" identified 124,383 vulnerabilities. The most recent 400 vulnerabilities since the prior 4/22/2021 assurance maintenance search were examined.

Identifier	Description	Analysis	Conclusion
N/A	The identified vulnerabilities were not related to the TOE nor did they appear to be relevant to the TOE.	The most recent 400 CVE entries were examined. In these entries Palo Alto was not identified. The respective entries involving HTTPS did not appear to be relevant to the TOE.	The TOE is not vulnerable.

Search Term: = TLS

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "TLS" returned ten new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A	The identified vulnerabilities were not related to the TOE nor did they appear to be relevant to the TOE.		The TOE is not vulnerable.

Search Term: = N/A

The latest vulnerabilities at the vendor website: https://securityadvisories.paloaltonetworks.com.

One vulnerability was identified since the prior 4/22/2021 assurance maintenance was examined.

Identifier	Description	Analysis	Conclusion
PAN-SA-2021-0003	The Palo Alto Networks Product Security Assurance team evaluated the NAME:WRECK DNS vulnerabilities impacting multiple TCP/IP software stack implementations. PAN-OS software and CloudGenix devices do not utilize the IPNet, Nucleus NET, FreeBSD, or NetX TCP/IP software stacks related to these vulnerabilities. As a result, there is no known security impact for these vulnerabilities in PAN-OS software or CloudGenix devices.	No PAN-OS products are affected.	The TOE is not vulnerable.

Search Term: = Cavium

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "Cavium" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A	The vulnerability search did not identify any new vulnerabilities since the 4/22/2021 search.		The TOE is not vulnerable.

Search Term: = VM-Series

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "VM-Series" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
	The vulnerability search did not identify any new vulnerabilities since the 4/22/2021 search.		The TOE is not vulnerable.

Search Term: = PAN-OS

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "PAN-OS" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
	The vulnerability search did not identify any new vulnerabilities since the 4/22/2021 search.		The TOE is not vulnerable.

Search Term: = Router

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "router" returned one new vulnerability since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A	The vulnerability was not related to the TOE nor did it appear to be relevant to the TOE.		The TOE is not vulnerable.

Search Term: = Switch

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "switch" returned nine new vulnerabilities since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	**Conclusion**
N/A	The vulnerabilities were not related to the TOE nor did it appear to be relevant to the TOE.		The TOE is not vulnerable.

Search Term: = Firewall

https://nvd.nist.gov/vuln/search

The search of the CVE database using the keyword "firewall" returned one new vulnerability since the prior 4/22/2021 assurance maintenance search.

Identifier	Description	Analysis	Conclusion
N/A	The vulnerability was not related to the TOE nor did it appear to be relevant to the TOE.		The TOE is not vulnerable.

Search Term: = UDP			
https://nvd.nist.gov/vuln/search The search of the CVE database using the keyword "UDP" returned eight new vulnerability since the prior 4/22/2021 assurance maintenance search.			
Identifier	**Description**	**Analysis**	**Conclusion**
N/A	The vulnerability was not related to the TOE nor did it appear to be relevant to the TOE.		The TOE is not vulnerable.

Search Term: = IPv4			
https://nvd.nist.gov/vuln/search The search of the CVE database using the keyword "IPv4" returned two new vulnerability since the prior 4/22/2021 assurance maintenance search.			
Identifier	**Description**	**Analysis**	**Conclusion**
N/A	The TOE was not identified in any of the matching records. The vulnerabilities are specific to other vendor's implementations.		The TOE is not vulnerable.

Search Term: = IPv6			
https://nvd.nist.gov/vuln/search The search of the CVE database using the keyword "IPv4" returned two new vulnerability since the prior 4/22/2021 assurance maintenance search.			
Identifier	**Description**	**Analysis**	**Conclusion**
N/A	The TOE was not identified in any of the matching records. The vulnerabilities are specific to other vendor's implementations.		The TOE is not vulnerable.

Search Term: = IPsec			
https://nvd.nist.gov/vuln/search The search of the CVE database using the keyword "IPsec" did not identify any new vulnerabilities since the prior 4/22/2021 assurance maintenance search.			
Identifier	**Description**	**Analysis**	**Conclusion**
N/A	The vulnerability search did not identify any new vulnerabilities since the 4/22/2021 search.		The TOE is not vulnerable.

In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version update. The IAR contains an extensive list of Issues, in Section 6, of the issues that were addressed.

Vendor Conclusion

The specific changes made to the firmware minor version and the addition of the Network Processing Card, PA-7000-DPC-A do not affect the security claims in the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.0 Security Target.

No updates or changes have been made to the Cryptographic Module. Therefore, the CAVP

certificates are still valid.

This update results in no changes to SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment and therefore is a minor change. The security target and the Common Criteria Evaluation Guidance Document are updated to reflect the firmware minor version update and the removal of the PA-3000 series firewalls.

Validation Team Conclusion

The Validation team has reviewed the changes and concurs that the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cider version of this product.