CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT
ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.2

Maintenance Update of Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0

Maintenance Report Number: CCEVS-VR-VID11284-2023-2

Date of Activity: September 13, 2023

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." August 29, 2014

Common Criteria document "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [NDcPP]

PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 [FW-Module]

PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 [VPNGW-Module]

Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v10.2 Security Target, Version 1.0, February 6, 2023

Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 Security Target, Version 1.0, August 8, 2023

Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v10.2 Impact Analysis Report, Version 1.0, August 8, 2023

PAN-OS Release Notes 11.0.2

Affected Evidence:

Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 Security Target, Version 1.0, August 8, 2023

Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next Generation Firewalls with PAN-OS 11.0, August 8, 2023

Updated Developer Evidence:

Security Target: Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 Security Target, Version 1.0, August 8, 2023

Changes in the maintained ST are:

- Document Title - Updated to enumerate specific covered models, consistent with other Palo Alto Networks evaluations.
- Section 1 - Updated TOE identification
- Section 1.1 - Updated identification of ST
- Section 1.1 - Updated TOE identification
- Section 2.1 - Updated TOE identification
- Section 2.2.1 – Updated the PAN-OS version number and TOE identification; removed the PA-220 hardware appliance; added the PA-415, PA-445, PA-1400 Series, and PA-5440 hardware appliances.
- Table 1 – Removed the PA-220 hardware appliance; added the PA-415, PA-445, PA-1400 Series, and PA-5440 hardware appliances.
- Section 2.3 – Identified the most current documentation for the current PAN-OS 11.0 release.
- Section 6.1 – removed reference to PA-220 appliance.
- Section 6.2 – updated CAVP certificate numbers.

Guidance Documentation: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next Generation Firewalls with PAN-OS 11.0, June 9, 2023

Changes in the maintained Guidance are:

- Document Title – Updated TOE version and document date
- Section 1.2 TOE References – Updated the version to 11.0.1; removed PA-220 model; added PA-415, PA-445, PA-1400 Series, and PA-5440 models.
- Section 1.3 Documentation References – Updated and identified the current documentation set for the 11.0 release.
-

Description of ASE Changes:

Palo Alto Networks submitted an Impact Analysis Report (IAR #1) to CCEVS for approval to the product updates for the Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 which are:

- Introduction of the PA-415 and PA-445 to the PA-400 Series hardware appliances running PAN-OS 11.0
- Introduction of the PA-5440 to the PA-5400 Series hardware appliances running PAN-OS 11.0
- Introduction of the PA-1400 Series (comprising the PA-1410 and PA-1420) hardware appliances running PAN-OS 11.0 to the Palo Alto next-generation firewall product line
- Removal of the PA-220 hardware appliance from the PA-220 Series hardware appliances
- Updating the firmware running on the Palo Alto next-generation firewall hardware appliances and the software of the next-generation virtual appliances from PAN-OS 10.2 to PAN-OS 11.0. The software updates included new non-security relevant features and bug fixes.
- Updating the CAVP certificates for cryptographic algorithms implemented by the Palo Alto Networks Crypto Module, to account for minor updates to the cryptographic module itself that addressed published vulnerabilities.

Description of ALC Changes:

The titles of the following documents were modified:

- Security Target

  Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.2 Security Target, Version 1.0, February 6, 2023

  TO

  Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 Security Target, Version 1.0, August 8, 2023

- Common Criteria Evaluated Configuration Guide (CCECG)

  Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next Generation Firewalls with PAN-OS 10.2, February 6, 2023

  TO

  Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next Generation Firewalls with PAN-OS 11.0, June 9, 2023

Description of Certificate changes

Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for all hardware and virtual appliances, including the new appliances added to the TOE (A3453 for hardware and A3454 for virtual appliances).

The Palo Alto Networks Crypto Module included with PAN-OS is substantially the same between versions 10.2 and 11.0. The only differences are patches made to address specific published vulnerabilities. The CAVP certificates for PAN-OS 11.0 of the Palo Alto Networks Crypto Module that is included with PAN-OS 11.0 cover the same set of functions and algorithms as obtained for PAN-OS 10.2.

The Operating environments (OEs) for the hardware appliances A2906 for v10.2 and A3453 for v11.0 are identical. Each processor used as a platform in the OE for A3453 has an exact match in the OE for A2906.

The OEs for these virtual platforms for A3454 are identical to those for A2907. The OEs for the virtual appliances (A2907 for v10.2, A3454 for v11.0), the following differences are noted:

- The processors used with AWS EC2 and Azure differ between A2907 (Intel Xeon E5 (Ivy Bridge)) and A3454 (Intel Xeon Platinum) and the processor microarchitectures used with AWS EC2 and Azure are not identified in the OE for A3454
- The processor used with GCP differs between A2907 (Intel Xeon 2.2 GHz (Skylake)) and A3454 (Intel Xeon Gold 6248 (Cascade Lake)).

However, these differences are not relevant because the AWS EC2, Azure, and GCP platforms are not in the evaluated configuration for the PAN-OS VM-Series.

The evaluation evidence presented by Palo Alto Networks for the v11.0 of the Palo Alto Networks Crypto Module that is included with Panorama 11.0 that cover the same set of functions and algorithms as obtained for v10.2.

The updated certificates were reviewed and approved by NIAP.

Changes to TOE:

The changes described in the IAR constitute all changes made to the Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v10.2 TOE since the previous assurance maintenance activity (CCEVS-VR-VID11284-2023).

- Introduction of the PA-415 and PA-445 to the PA-400 Series hardware appliances running PAN-OS 11.0
- Introduction of the PA-5440 to the PA-5400 Series hardware appliances running PAN-OS 11.0
- Introduction of the PA-1400 Series (comprising the PA-1410 and PA-1420) hardware appliances running PAN-OS 11.0 to the Palo Alto next-generation firewall product line
- Removal of the PA-220 hardware appliance from the PA-220 Series hardware appliances
- Updating the firmware running on the Palo Alto next-generation firewall hardware appliances and the software of the next-generation virtual appliances from PAN-OS 10.2 to PAN-OS 11.0. The software updates included new non-security relevant features and bug fixes.
- Updating the CAVP certificates for cryptographic algorithms implemented by the Palo Alto Networks Crypto Module, to account for minor updates to the cryptographic module itself that addressed published vulnerabilities.

Category		Number of Changes	Applicability to New Firmware Versions
Performance Improvements		16	All 16 features improved performance without affecting security functionality.
Non-Security-Relevant Features and Feature Enhancements		6	Six of the software updates of the next-generation virtual appliances from PAN-OS 10.2 to PAN-OS 11.0 were non-security relevant features and enhancements like Increased Maximum Number of Security Zones for PA-3400 Series Firewalls, Multi-Vsys Capability for the PA-400 Series Firewalls, and soon
Non-SFR-related (Security - Relevant) Features and Feature Enhancements		18	18 of the software updates/new features applied were outside the TOE boundary, disabled by default in the evaluated configuration, and/or applied to Panorama and not Palo Alto Networks firewall running PAN-OS. These features include WEB PROXY,TLSv1.3 Support for Management Access, Advanced Routing Engine support on CN-Series and soon
Bug Fixes	Performance Improvement	90	204 Bug Fixes were made for issues identified in previous releases. The bug fixes were behavioral and performance Bug Fixes and not security relevant (CVE) Fixes. The bug-fixes did not result in changes to the ST or guidance documentation. These changes were either unrelated to SFR testing or were not visible at the level of testing performed for the SFRs. Thus, the original testing still holds, and any fix testing was covered by vendor non-evaluation regression and checkout testing.
	Behavior Corrections	67	
	Outside the Scope of Evaluation/ Not related to the TOE	47	

Assurance Continuity Maintenance Report:

The Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 Impact Analysis Report was sent to CCEVS for approval in August, 2023. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, “Assurance

Continuity: CCRA Requirements", version 1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, and the ST and Guidance Documentation were updated as a result of the changes and the security impact of the changes.

Description of Regression Testing:

Palo Alto Networks regression test results were produced and found consistent with the previous test results. Palo Alto performs extensive regression testing for every release including 10.2. Palo Alto conducts automation test suites and also performed manual testing.

Vulnerability Assessment:

Palo Alto Networks searched the Internet for potential vulnerabilities in the TOE using the three public vulnerability repositories listed below.

- NIST National Vulnerabilities Database (http://web.nvd.nist.gov)
- US-CERT (http://www.kb.cert.org)
- Palo Alto Networks Security Advisories (https://security.paloaltonetworks.com/).

Palo Alto Networks PAN-OS 11.0 selected key words based upon the vendor's name, product names, and key platform features the product leverages including processors, processor microarchitectures, and software. The search terms used were:

- "Palo Alto Firewall", "Palo Alto Networks Firewall", "PA-220 Series", "PA-400 Series", "PA-800 Series", "PA-1400 Series", "PA-3200 Series", "PA-3400 Series" , "PA-5200 Series", PA-5400 Series", "PA-5450", "PA-7000 Series", and "VM-Series" as variations of the TOE name.
- Processors:
    - AMD EPYC 7352
    - AMD EPYC 7452
    - AMD EPYC 7642
    - AMD EPYC 7742
    - Cavium Octeon CN7130
    - Cavium Octeon CN7240
    - Cavium Octeon CN7350
    - Cavium Octeon CN7360
    - Cavium Octeon CN7885
    - Cavium Octeon CN7890
    - Intel Atom C5325
    - Intel Atom C5335C1
    - Intel Atom C3436L
    - Intel Atom C3558R
    - Intel Atom C3758R
    - Intel Atom P5332
    - Intel Atom P5342
    - Intel Atom P5352
    - Intel Atom P5362
    - Intel Pentium D1517
    - Intel Xeon D-1548
    - Intel Xeon D-1567

    - Intel Xeon D-2187NT
    - Intel Core i7-2715QE
    - Intel Xeon Gold 6248
- Processor microarchitectures:
    - MIPS64
    - Skylake
    - Cascade Lake
    - Ivy Bridge
    - Haswell
    - Broadwell
    - Goldmont
    - Denverton
    - Tremont
    - Snow Ridge
    - Zen 2
    - Sandy Bridge
- Software:
    - PAN-OS 11.0

The IAR contains the output from the vulnerability searches published since April 26, 2023, the rationale why the search results are not applicable to the TOE, and the search results of newly added search terms. This search was performed on September 12, 2023. No vulnerabilities affecting the TOE were found.

(They considered results dated after April 26, 2023, when the evaluation team conducted the final vulnerability searches for PAN-OS 10.2, plus the search results of newly added search terms)

Vendor Conclusion:

The addition of new hardware appliances (PA-415, PA-445, PA-1410, PA-1420, PA-5440), removal of the PA-220 hardware appliance, and the specific changes made to the firmware version do not affect the security claims in the Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0 Security Target.

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.

Palo Alto Networks performs extensive regression testing on all releases, utilizing automation test suites. Palo Alto Networks found the regression test results for 11.0 to be consistent with the test results for previous versions.

Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for all hardware and virtual appliances, including the new appliances added to the TOE (A3453 for hardware and A3454 for virtual appliances).

Finally, the analyst searched the public domain for any new potential vulnerabilities that may have been identified since the completion of the previous maintenance activity. The search did not identify any new potential vulnerability.

Validation Team Conclusion:

The validation team reviewed the changes and concur the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The Security Target was updated to reflect the new version and the admin guidance was updated to include small editorial changes/clarifications. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.