CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT
ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

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

Maintenance Update of 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

Maintenance Report Number: CCEVS-VR-VID11284-2023

Date of Activity: April 26, 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 1.1, 18 June 2020 [VPNGW-Module]

Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 Security Target, Version 1.1, August 31, 2022

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 Impact Analysis Report, Version 1.1, April 26, 2023

PAN-OS Release Notes 10.2.3-h2
PAN-OS 10.2.3-h1 Hotfix Release Notes

Affected Evidence:

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

Updated Developer Evidence:

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

Changes in the maintained ST are:

- Section 1.1 - Updated identification of ST
- Section 1.1 - Updated TOE Identification (new devices and software version)
- Section 2.1 - Updated TOE identification
- Section 2.2.1 – Updated the PAN-OS version number; added the PA-3400 Series and PA-5400 Series hardware appliances
- Section 2.3 – Identified the most current documentation for the current PAN-OS release 10.2
- 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 10.2, February 6, 2023

Changes in the maintained Guidance are:

- Section 1.2 TOE References – Updated the version to 10.2.3-h1; added PA-3400 Series and PA-5400 Series devices
- Section 1.3 Documentation References – Updated and identified the current documentation set for the 10.2 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-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, which are:

- Introduction of the PA-3400 Series (comprising the PA-3410, PA-3420, PA-3430, and PA-3440 appliances) and PA-5400 Series (comprising the PA-5410, PA-5420, and PA-5430 appliances) hardware appliances running PAN-OS 10.2 to the Palo Alto next-generation firewall product line
- Removal of the following PA-7000 line cards, which do not support the 10.2 firmware: PAN-PA-7050-SMC; PAN-PA-7080-SMC; PAN-PA-7000-20GXM-NPC; and PAN-PA-7000-20GQXM-NPC

- 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 10.1 to PAN-OS 10.2. 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, and to accommodate new operational environments introduced with the PA-3400 Series and PA-5400 Series appliances

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-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 Security Target, Version 1.1, August 31, 2022
  TO
  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

- Common Criteria Evaluated Configuration Guide (CCECG)
  Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next Generation Firewalls with PAN-OS 10.1, August 31, 2022
  TO
  Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next Generation Firewalls with PAN-OS 10.2, February 6, 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 (A2906 for hardware and A2907 for virtual appliances). The Operating environment for A2907 is identical to the operating environment for A2244.

The Palo Alto Networks Crypto Module included with PAN-OS is substantially the same between versions 10.1 and 10.2. The only differences are patches made to address specific published vulnerabilities. The CAVP certificates for v10.2 of the Palo Alto Networks Crypto Module that is included with PAN-OS 10.2 cover the same set of functions and algorithms as obtained for v10.1.

The evaluation evidence presented by Palo Alto Networks for the CAVP certificates from the TOE's original ETR and the evidence for the CAVP certificates for the updated TOE provided equivalence rationale to address any apparent differences between the two sets of certificates.

NIAP reviewed and verified that the CAVP cert changes are not considered major changes and they are the same in the relevant areas to the original certificates. The changes that resulted in the need for new crypto certs do not require a rerun in any of the testing assurance activities.

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 10.1 TOE since the previous Common Criteria evaluation (CCEVS-VR-VID11284-2022).

- Introduction of the PA-3400 Series (comprising the PA-3410, PA-3420, PA-3430, and PA-3440 appliances) and PA-5400 Series (comprising the PA-5410, PA-5420, and PA-5430 appliances) hardware appliances running PAN-OS 10.2 to the Palo Alto next-generation firewall product line
- Removal of the following PA-7000 line cards, which do not support the 10.2 firmware: PAN-PA-7050-SMC; PAN-PA-7080-SMC; PAN-PA-7000-20GXM-NPC; and PAN-PA-7000-20GQXM-NPC
- 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 10.1 to PAN-OS 10.2. The software updates included new non-security relevant features and bug fixes. The PAN-OS updates listed below are reviewed with respect to the PAN-OS next-generation firewall evaluation.
- 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, and to accommodate new operational environments introduced with the PA-3400 Series and PA-5400 Series appliances.

Category	Number of Changes	Applicability to New Firmware Versions
Performance Improvements	8	All 8 Performance Improvements were included in all the new firmware versions.
New Features and Feature Enhancements	27	The software updates of the next-generation virtual appliances from PAN-OS 10.1 to PAN-OS 10.2.3 were non-security relevant features and enhancements like advanced routing engine, new BGP capabilities, new OSPFv3 and OSPFv2 capabilities and so on.
Bug Fixes	215	215 Bug Fixes were made for issues identified in previous releases of which two were security relevant (CVE) Fixes and 213 were behavioral Bug Fixes. The bug-fixes did not result in changes to the ST or guidance documentation and had no effect on the result of any Assurance Activity test.

Assurance Continuity Maintenance Report:

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 Impact Analysis Report was sent to CCEVS for approval in February, 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 10.1 selected key words based upon the vendor's name, product names, and key platform features the product leverages including processors, processor microarchitectures, software, and protocols. The search terms used were:

- "Palo Alto Firewall", "Palo Alto Networks Firewall", "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" as variations of the TOE name.
- Processors:
  - AMD EPYC 7352
  - AMD EPYC 7452
  - AMD EPYC 7642
  - Cavium Octeon CN7130
  - Cavium Octeon CN7240
  - Cavium Octeon CN7350
  - Cavium Octeon CN7360
  - Cavium Octeon CN7885
  - Cavium Octeon CN7890
  - 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 10.2
- Protocols (note, since these protocols are pervasive in IT products, there is little value in attempting to search vulnerability repositories such as the NVD using just the protocol (e.g., "TCP"). Such a search produces thousands of results, the vast majority of which are specific to a particular product that is unrelated to the TOE. Therefore, when searching public vulnerability repositories, the evaluation team includes the vendor's name):
    - TCP
    - UDP
    - IPv4
    - IPv6
    - TLS
    - SSH
    - HTTPS
    - IPsec.

The IAR contains the output from the vulnerability searches published since August 4 2022 and the rationale why the search results are not applicable to the TOE. This search was performed on April 26, 2023. No vulnerabilities affecting the TOE were found.

(They considered results dated after August 4, 2022, when the evaluation team conducted the final vulnerability searches for PAN-OS 10.1.)

Vendor Conclusion:

The addition of the PA-3400 Series and PA-5400 Series hardware appliances and the specific changes made to the firmware/software do not affect the security claims in 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 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.

Vendor 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.

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 (A2906 for hardware and A2907 for virtual appliances). NIAP reviewed and verified that the CAVP cert changes are not considered major changes and they are the same in the relevant areas to the original certificates. The changes that resulted in the need for new crypto certs do not require a rerun in any of the testing assurance activities.

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.

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.