National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks Panorama v8.1.10

Report Number: CCEVS-VR-VID10980-2019
Dated: 12 November 2019
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements

Validation Team

James Donndelinger

Marybeth Panock

Tony Chew

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1. Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Palo Alto Networks Panorama v8.1.10 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Palo Alto Networks Panorama v8.1.10 (Panorama) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in October 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for NDcPP v2.1.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5.) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the NDcPP v2.1 This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to provide oversight of the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Palo Alto Networks Panorama v8.1.10
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
Security Target	Palo Alto Networks Panorama v8.1.10 Security Target, Version 1.0, August 27, 2019
Evaluation Technical Report	• Evaluation Technical Report for Palo Alto Networks Panorama v8.1.10 Part 1 (Non-Proprietary) Version 1.2, October 18, 2019 • Evaluation Technical Report for Palo Alto Networks Panorama v8.1.10 Part 2 (Palo Alto Proprietary) ETR Version 1.2 October 18, 2019
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Palo Alto Networks
Developer	Palo Alto Networks
Common Criteria Testing Lab (CCTL)	Leidos
CCEVS Validators	James Donndelinger, Marybeth Panock, and Tony Chew

3. Architectural Information

TOE Architecture

The TOE high-level architecture is divided into four main subsystems: system software (SS); database (DB); hardware (HW) and the hardened Linux-Derived operating system (OS). The system software provides system management functionality including proprietary software, management interfaces (CLI and GUI), cryptographic support (Palo Alto Networks Crypto Module), logging service (syslog-ng and auditd), web service (nginx), and authentication service. The database provides a data repository for audit logs, user account data, system data, configuration data, system log (i.e., syslog), and configuration logs. The operating system provides a customized Linux kernel to enforce domain separation, memory management, disk access, file I/O, network stacks (IPv4/IPv6), and communications with the underlying hardware components including the network interface cards (NICs), memory, CPUs, and hard disks. Only services and libraries required by the system software and DB are enabled in the OS. The virtual appliances will include the hypervisor as well (not shown in figure 1).

The following diagram depicts both the hardware and software architecture of the TOE.

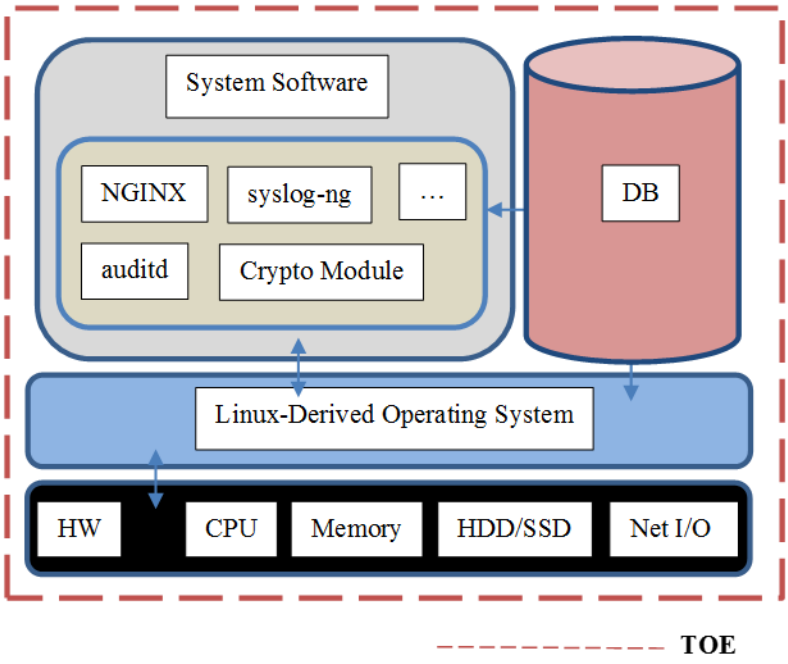

Figure 1 TOE Architecture

4. Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the ETR.

Security Audit

The TOE is designed to be able to generate logs for security relevant events including the events specified in the claimed PP. By default, the TOE stores the logs locally so they can be accessed by an administrator. The TOE can also be configured to send the logs securely to a designated external log server.

Cryptographic Support

The TOE implements NIST-validated cryptographic algorithms that provide key management, random bit generation (RBG), encryption/decryption, digital signature generation and verification, cryptographic hashing, and keyed-hash message authentication features in support of higher level cryptographic protocols, including SSH and TLS. Note that to be in the evaluated configuration, the TOE must be configured in FIPS-CC mode, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard and the claimed PP.

Identification and Authentication

The TOE requires all users accessing the TOE user interfaces to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers network accessible (HTTP over TLS, SSH) and direct connections to the GUI and SSH for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition and authentication of administrators with username, password, and role (set of privileges), which it uses to authenticate the human user and to associate that user with an authorized role. In addition, the TOE can authenticate users using X509 certificates and can be configured to lock a user out after a configurable number of unsuccessful authentication attempts.

Security Management

The TOE provides a GUI or CLI to access the security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE. The TOE provides access to the GUI/CLI locally via direct RJ-45 Ethernet cable connection and remotely using an HTTPS/TLS or SSHv2 client.

The TOE provides a number of management functions and restricts them to users with the appropriate privileges. The management functions include the capability to configure the audit function, configure the idle timeout, and review the audit trail. The TOE provides pre-defined Security Administrator, Audit Administrator, and Cryptographic Administrator roles. These administrator roles are all considered Security Administrator as defined in the claimed PP for the purposes of this ST.

Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE includes functions to perform self-tests so that it can detect when it is failing. It also includes mechanism to verify TOE updates to prevent malicious or other unexpected changes in the TOE.

TOE Access

The TOE provides the capabilities for both TOE- and user-initiated locking of interactive sessions and for TOE termination of an interactive session after a period of inactivity. The TOE will display an advisory and consent warning message regarding unauthorized use of the TOE before establishing a user session.

Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH or HTTP over TLS (HTTPS). SSH and TLS ensure both integrity and disclosure protection.

The TOE protects communication with the syslog server, Palo Alto Networks firewalls and Wildfire Appliances using TLS connections.

5. Assumptions and Clarification of Scope

Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, are as follows:

- The device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.
- The device is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent of the functionality that is evaluated for conformance to the NDcPP is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data.
- The authorized administrators for the device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
- The device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.
- It is assumed that the administrator will ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Evaluation Activities for Network Device cPP* [6] and performed by the evaluation team).
- This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Palo Alto Networks Panorama v8.1.10 Security Target, Version 1.0, August 27, 2019 [7]. Section 2.4 of [7] lists the specific features that were excluded from the evaluation.

- The TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.
- In a deployment architecture, the Panorama security management appliance provides the capability to remotely manage multiple firewall appliances that control network traffic flow and WildFire appliances that analyze suspicious files traversing the network. However, since the firewall and Wildfire appliances are in the operational environment, these capabilities (i.e., stateful inspection filtering, IPsec VPN gateway, IPS/IDS threat prevention) are not evaluated (out of scope). Only the secure communication channels from Panorama to firewalls and Wildfires are claimed.

6. Documentation

Palo Alto offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with each TOE model is as follows:

- Panorama Administrator's Guide, Version 8.1, March 26, 2019 [8]
- VM-Series Deployment Guide, Version 8.1, May 6, 2019 [9]
- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama v8.1, Version 1.0, August 26, 2019 [10]

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in these guides.

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download this CC configuration guide (CCECG above) from the NIAP website. TOE Evaluated Configuration

7. TOE Evaluated Configuration

Evaluated Configuration

The TOE is the Palo Alto Networks Panorama, Version 8.1.10, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report. The specific appliance models include:

- M-100
- M-200
- M-500
- M-600
- Panorama Virtual Appliance

If used, the Virtual Appliance must be the only guest running in the virtualized environment, in accordance with the requirements of the NDcPP.

The TOE includes a "FIPS-CC" mode of operation. This mode must be enabled for the TOE to meet the claimed requirements.

Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the NDcPP is excluded from the evaluation scope. The product also has the following exclusions:

- Telnet and HTTP Management Protocols: Telnet and HTTP are disabled by default and cannot be enabled in the evaluated configuration. Telnet and HTTP are insecure protocols which allow for plaintext passwords to be transmitted. Use SSH and HTTPS only as the management protocols to manage the TOE.
- External Authentication Servers: The NDcPP does not require external authentication servers.
- Shell and Console Access: The shell and console access is only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting.
- REST API: This feature is not evaluated as part of the evaluation. REST API relies on HTTPS as the underlying communication protocol and can be used to build a management interface. This feature is not tested and is out of scope.
- Stateful inspection filtering, VPN gateway, IPS/IDS threat prevention, URL filtering (PAN-DB), Log forwarding, and Malware sandboxing: These features are provided by Palo Alto Networks firewalls and Wildfire appliances and are not included in this evaluation. Only the secure TLS connections between the firewalls and Wildfire to the TOE were evaluated.
- Centralized Device Management: These features (e.g., Policy Template and Push, Device Group) were not evaluated. Only the secure TLS connections between the firewalls and Wildfire to the TOE were evaluated.

8. Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary documents:

- *Palo Alto Panorama Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.1* [11]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for Palo Alto Panorama [12]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Network Devices* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *collaborative Protection Profile for Network Devices* [5]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* [5] were fulfilled.

Test Configuration

The evaluated version of the TOE consists of Palo Alto Panorama version 8.1.10 running on any of the following physical and virtual appliances:

- M-100
- M-200
- M-500
- M-600
- Panorama Virtual Appliance

The TOE must be deployed as described in section 5 “Assumptions” of this Validation Report and be configured in accordance with the *Panorama Administrator’s Guide* [8], *VM-Series Deployment Guide* [9], and *Palo Alto Networks Common Criteria Evaluate Configuration Guide (CCECG) for Panorama v8.1* [10].

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

9. Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- *Evaluation Activities for Network Device cPP*, Version 2.1, September 2018 [6]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profiles and using the flaw-hypothesis methodology. This included a search of public vulnerability databases and development of Type 3 flaw hypotheses in accordance with Section A.3 of

[6]. These searches were performed during the evaluation on July 26, 2019 to ensure that no additional public vulnerabilities were disclosed prior to the completion of the evaluation.

The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and several other public vulnerability repositories. Searches were performed on 7/26/2019.

The keyword searches included the following terms:

- "Palo Alto"
- "Panorama"
- "PAN-OS"
- "Management Appliance"
- "TCP"
- "SSH"
- "HTTPS"
- "TLS"
- "Microarchitectural"
- "Linux 3.10"

The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

10. Validator Comments/Recommendations

The product supports many features and protocols that are not evaluated or must be disabled in the evaluated configuration. This is documented in the "Excluded Functionality" paragraph of section 7 "TOE Evaluated Configuration", in the Security Target, and in the CC Guide [10]. It is reiterated here because it is an extensive list. The only protocols implemented by the TOE that have been tested to the extent specified by the security functional requirements are the secure TLS connections between the firewalls and Wildfire to the TOE, HTTPS, and SSH. The excluded protocols include

- Telnet and HTTP Management Protocols
- External Authentication Servers
- Shell and Console Access
- REST API
- Stateful inspection filtering, VPN gateway, IPS/IDS threat prevention, URL filtering (PAN-DB), Log forwarding, and Malware sandboxing:
- Centralized Device Management: These features (e.g., Policy Template and Push, Device Group) were not evaluated.

All other items and scope issues have been sufficiently addressed elsewhere in the document.

11. Annexes

Not applicable

12. Security Target

The ST for this product's evaluation is *Palo Alto Networks Panorama Security Target*, Version 1.0, 27 August 2019 [7].

13. Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

14.Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017
3. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017
5. collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
6. Evaluation Activities for Network Device cPP, Version 2.1, September 2018
7. Palo Alto Networks Panorama v8.1.10 Security Target, Version 1.0, August 27, 2019 (ST)
8. Panorama Administrator's Guide, Version 8.1, March 26, 2019
9. VM-Series Deployment Guide, Version 8.1, May 6, 2019
10. Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama v8.1, Version 1.0, August 26, 2019 (AGD)
11. Palo Alto Panorama Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.1, Version 1.1 September 9, 2019 (DTR)
12. Assurance Activities Report for Palo Alto Panorama, Version 1.2, October 18, 2019 (AAR)
13. Evaluation Technical Report for Palo Alto Networks Panorama v8.1.10 Part 1 (Non-Proprietary) Version 1.2, October 18, 2019 (ETR P1)
14. Evaluation Technical Report for Palo Alto Networks Panorama v8.1.10 Part 2 (Palo Alto Proprietary) ETR Version 1.2 October 18, 2019 (ETR P2)