National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Palo Alto Networks M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.0

Report Number: CCEVS-VR-VID11070-2020
Dated: August 17, 2020
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 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Jenn Dotson

Sheldon Durrant (Senior Validator)

Randy Heimann

Lisa Mitchell

Linda Morrison (Lead Validator)

Clare Olin

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 5 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 M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.0 (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 M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.0 (Panorama) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2020.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following document:

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

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The product comprises network appliances and virtual appliances on specified hardware used to facilitate threat protection, shield computing infrastructure from network vulnerabilities, block exploits, and defend against known and zero-day attacks. The focus of the evaluation was on the product's conformance to the security functionality specified in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 [5]

The security functions specified in this Protection Profile include protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [7]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([12]) and the associated test report produced by the Leidos evaluation team ([11]).

The validation team reviewed the evaluation outputs produced by the evaluation team, the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6] had been performed appropriately. Therefore, 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 and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Compliant List (PCL).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Palo Alto Networks M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.0
Sponsor & Developer:	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	August 17, 2020
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Pascal Patin Greg Beaver
Validation Personnel:	Jenn Dotson Sheldon Durrant Randy Heimann Lisa Mitchell Linda Morrison Clare Olin

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target. The TOE is one or more Palo Alto Networks management appliance(s) that include Panorama M-100, M-200, M-500 and M-600 appliances and virtual appliances all running version 9.0.9.

3.1 TOE Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 6 below.

3.2 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.

3.3 Physical Boundaries

The TOE consists of the following components:

- Hardware appliance-includes the physical port connections on the outside of the appliance cabinet and a time clock that provides the time stamp used for the audit records.
- Virtual appliances installed on specified hardware - the VM-Series supports the exact security functionalities available in the physical form factor appliances, allowing an administrator to safely enable physical or virtual appliances that enable applications flowing into, and across your virtual computing environments. The VM software and the appliances are both included in the TOE. The time clock, as well as CPU, ports, etc., are provided by VM environment (hypervisor) hosting the VMs. VMs are deployed in the system using Intel CPUs.
- Panorama OS software v9.0.9 – the software/firmware component that runs the appliance. For VMs, Panorama OS is software and for hardware appliances, Panorama OS is firmware. Panorama OS is built on top of a Linux kernel and runs along with NGINX (the web server that Palo Alto Networks uses), syslog-ng, sshd, Palo Alto Networks Crypto Module, and various vendor-developed applications that implement its capabilities.

The physical boundary of the TOE comprises the whole appliance (M-100, M-200, M-500, and M-600); and the virtual appliances on specified hypervisor and hardware. The models only differ in their performance capability (e.g., processor speed, memory, and disk space), but they all provide the same security functionality.

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.

4.1 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.

4.2 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.

4.3 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.

4.4 Security Management

The TOE provides a GUI, CLI, or API (XML and REST) 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 [NDcPP] for the purposes of this ST.

4.5 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.

4.6 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.

4.7 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

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

That information has not been reproduced here and the NDcPP21 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP21 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.2 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 v9.0 Security Target, Version 1.0, June 26, 2020 [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 7 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 TOE Evaluated Configuration

6.1 Evaluated Configuration

The TOE is the Palo Alto Networks Panorama, Version 9.0.9, as configured in accordance with the guidance documentation listed in Section 7 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.

6.2 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.

7 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 9.0, March 12, 2020[8]
- VM-Series Deployment Guide, Version 9.0, December 2. 2019 [9]
- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 9.0, April 29, 2020 [10]
- PAN-OS and Panorama API Usage Guide, Version 9.0, April 17, 2020 [13]

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 the CC configuration guide (CCECG above) from the NIAP website.

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 9.0.9 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 3.1 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 v9.0* [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.

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].

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 8/5/2020.

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.

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

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECC) for Panorama 9.0, April 29, 2020.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The ST for this product's evaluation is *Palo Alto Networks Panorama 9.0 Security Target,* Version 1.0, June 26, 2020 [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 9.0 Security Target, Version 1.0, June 26, 2020

[8] Panorama Administrator's Guide Version 9.0, March 12, 2020

[9] VM-Series Deployment Guide, Version 9.0, December 2, 2019

[10] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 9.0, April 29, 2020

[11] Palo Alto Panorama Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.1, document Version 1.1, June 26, 2020

[12] Assurance Activities Report For Palo Alto Networks Panorama 9.0.9, Version 1.0, June 26, 2020

[13] PAN-OS and Panorama API Usage Guide, Version 9.0, April 17, 2020