

**National Information Assurance Partnership**

**Common Criteria Evaluation and Validation Scheme**



**Validation Report**

**for**

**Palo Alto Networks M-200, M-300, M-600, and M-700  
Hardware, and Virtual Appliances all running Panorama 11.1**

**Report Number: CCEVS-VR-VID11500-2025**  
**Dated: 19 May 2025**  
**Version: 1.0**

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

Department of Defense  
ATTN: NIAP, Suite 6982  
9800 Savage Road  
Fort Meade, MD 20755-6982

## VALIDATION REPORT

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1

---

### **Acknowledgements**

#### **Validation Team**

Jenn Dotson

Randy Heimann

Lisa Mitchell

Linda Morrison

Lori Sarem

*The MITRE Corporation*

#### **Common Criteria Testing Laboratory**

Leidos Inc.

Columbia, MD

## Contents

1	Executive Summary .....	4
2	Identification .....	5
3	Architectural Information.....	7
3.1	TOE Description .....	7
3.2	TOE Platforms .....	8
3.3	Physical Boundaries .....	9
4	Security Policy .....	11
4.1	Security Audit.....	11
4.2	Cryptographic Support.....	11
4.3	Identification and Authentication.....	11
4.4	Security Management.....	11
4.5	Protection of the TSF .....	12
4.6	TOE Access .....	12
4.7	Trusted Path/Channels .....	12
5	Assumptions and Clarification of Scope .....	13
5.1	Assumptions.....	13
5.2	Clarification of Scope .....	13
6	Documentation.....	14
7	IT Product Testing.....	15
7.1	Developer Testing .....	15
7.2	Evaluation Team Independent Testing .....	15
8	TOE Evaluated Configuration .....	16
8.1	Evaluated Configuration .....	16
8.2	Excluded Functionality .....	17
9	Results of the Evaluation .....	18
9.1	Evaluation of the Security Target (ASE) .....	18
9.2	Evaluation of the Development (ADV).....	18
9.3	Evaluation of the Guidance Documents (AGD).....	18
9.4	Evaluation of the Life Cycle Support Activities (ALC) .....	19
9.5	Evaluation of the Test Documentation and the Test Activity (ATE) .....	19

## VALIDATION REPORT

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1

---

9.6	Vulnerability Analysis .....	19
9.7	Summary of Evaluation Results .....	20
10	Validator Comments/Recommendations .....	21
11	Security Target.....	22
12	Abbreviations and Acronyms .....	23
13	Bibliography.....	24

## 1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) validation team's assessment of the evaluation of the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 provided by Palo Alto Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by the Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in May 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Leidos, Inc. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the:

- *collaborative Protection Profile for Network Device*, Version 3.0e, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG]

The TOE is the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). This VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 Security Target*, Version 1.0, March 20, 2025 and analysis performed by the validation team.

## 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 Validated Products 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 to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

<b>Evaluation Scheme:</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>Evaluated Product:</b>	Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1
<b>Sponsor &amp; Developer:</b>	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
<b>CCTL:</b>	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
<b>ST:</b>	<i>Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 Security Target, Version 1.0, March 20, 2025</i>
<b>ETR:</b>	<i>Evaluation Technical Report for Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1, Version 1.0, May 12, 2025</i>
<b>CC:</b>	<i>Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017</i>

# VALIDATION REPORT

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1

---

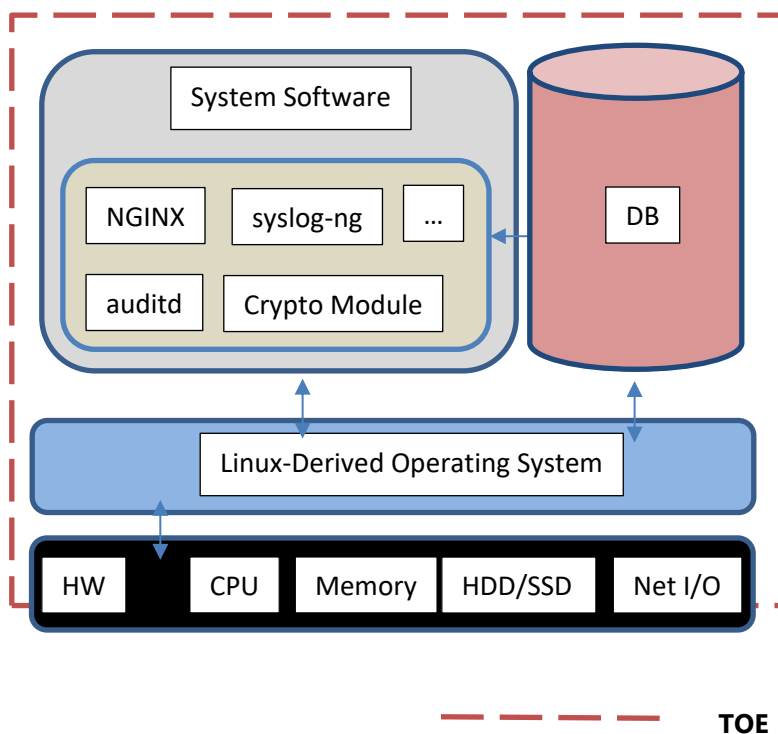
<b>CEM:</b>	<i>Common Methodology for Information Technology Security Evaluation</i> , Version 3.1, Release 5, April 2017
<b>Protection Profiles:</b>	<i>collaborative Protection Profile for Network Devices</i> , Version 3.0e, 6 December 2023  <i>Functional Package for Secure Shell (SSH)</i> , Version 1.0, 13 May 2021
<b>Conformance Result:</b>	CC Part 2 extended; CC Part 3 conformant
<b>Evaluation Personnel:</b>	Anthony Apted Greg Beaver Armin Najafabadi Kofi Owusu Pascal Patin Kevin Zhang
<b>Validation Personnel:</b>	Jenn Dotson Randy Heimann Lisa Mitchell Linda Morrison Lori Sarem

### 3 Architectural Information

Note, the following architectural description is based on the description presented in the ST.

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**

#### 3.1 TOE Description

Palo Alto Networks Panorama management appliance provides centralized monitoring and management of Palo Alto Networks next-generation firewalls and Wildfire appliances. It provides a single location from







## VALIDATION REPORT

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1

which administrators can oversee all applications, users, and content traversing the whole network, and then use this knowledge to create application enablement policies that control and protect the network.

### 3.2 TOE Platforms

Product Identification	Illustration	Description
M-200		<p>Processor: Intel Xeon E5-2620 v4 (Broadwell)</p> <p>Memory: 128 GB DDR4</p> <p>Maximum Log Storage on Appliance: 16 TB (4 8TB RAID disks)</p> <p>SSD Storage Space: 240 GB</p>
M-300		<p>Processor: Intel Xeon Silver 4310 (Ice Lake)</p> <p>Memory: 256 GB DDR4</p> <p>Maximum Log Storage on Appliance: 32 TB (4 x 8TB RAID disks)</p> <p>SSD Storage Space: 480 GB</p>
M-600		<p>Processor: Intel Xeon E5-2680 v4 (Broadwell)</p> <p>Memory: 256 GB DDR4</p> <p>Maximum Log Storage on Appliance: 48 TB (12 8TB RAID disks)</p> <p>SSD Storage Space: 240 GB</p>
M-700		<p>Processor: Intel Xeon Silver 4316 (Ice Lake)</p> <p>Memory: 512 GB DDR4</p> <p>Maximum Log Storage on Appliance: 48 TB (12 8TB RAID disks)</p> <p>SSD Storage Space: 480 GB</p>
<b>Virtual Appliances</b>		
On VMware ESXi		<p>Processor: See section 1.1.</p> <p>Memory: Up to 64 GB (min 16 GB)</p> <p>Maximum Logging Rate as Manager: 10,000 logs per second</p>

## VALIDATION REPORT

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1

Product Identification	Illustration	Description
		Maximum Log Storage on Appliance: 24 TB (12 virtual logging disks) SSD Storage Space: N/A
On Hyper-V		Processor: See section 1.1. Memory: Up to 32 GB (min 8 GB) Maximum Logging Rate as Manager: 10,000 logs per second Maximum Log Storage on Appliance: 24 TB (12 virtual logging disks) SSD Storage Space: N/A
On KVM		Processor: See section 1.1. Memory: Up to 32 GB (min 8 GB) Maximum Logging Rate as Manager: 10,000 logs per second Maximum Log Storage on Appliance: 24 TB (12 virtual logging disks) SSD Storage Space: N/A

### 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 their 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 v11.1 - 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

## VALIDATION REPORT

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1

---

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-200, M-300, M-600, and M-700); and the virtual appliances on specified hypervisors 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

This section summarizes the security functions provided by the TOE:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

### 4.1 Security Audit

The TOE is designed to generate audit records of security-relevant events including the events specified in [NDcPP] and [SSHPKG]. 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, encryption/decryption, digital signature generation and verification, and 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 standard and the PP claims.

### 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 interfaces via HTTPS (GUI) and SSH (CLI) for interactive administrator sessions and programmatic interfaces via HTTPS for XML and REST APIs.

The TOE supports the local (i.e., on device) definition and authentication of administrators with username, password or public-key, 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 the administrators have

provided acceptable user identification and authentication data to the TOE. The TOE provides access to the GUI/CLI 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].

#### 4.5 Protection of the TSF

The TOE implements mechanisms 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 and transitions to a secure maintenance state. It also includes a mechanism to verify TOE updates to prevent malicious or other unexpected changes in the TOE.

#### 4.6 TOE Access

The TOE can be configured to display an administrator-defined advisory banner before establishing an administrative user session and to terminate remote interactive sessions after a configurable period of inactivity. It also provides the capability for users to terminate their own interactive sessions.

#### 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 Device*, Version 3.0e, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG]

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

### 5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP/SSHPKG as described for this TOE in the ST. 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.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the Network Device Protection Profile with the Secure Shell Functional Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP/SSHPKG and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

## 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:

- *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 11.1*, Revision Date: March 20, 2025
- *Panorama Administrator's Guide Version 11.1*, Last Revised: August 19, 2024
- *PAN-OS and Panorama API Usage Guide, Version 11.1 & later*, Last Revised: August 21, 2024

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

## 7 IT Product Testing

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

- *Palo Alto Panorama v11.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 3.0e, Version 1.0, May 12, 2025*

A non-proprietary summary of the assurance activities is provided in the following document:

- *Assurance Activities Report for Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1, Version 1.0, May 12, 2025*

### 7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

### 7.2 Evaluation Team Independent Testing

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* and *Functional Package for Secure Shell (SSH)*.

The valuation team devised a Test Plan based on the Testing Assurance Activities specified in *Evaluation Activities for Network Device cPP* and *Functional Package for Secure Shell (SSH)*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The valuation 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 from October 2024 to May 2025.

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



## 8 TOE Evaluated Configuration

This section briefly identifies the evaluated configuration(s) and any excluded and out of scope functionality.

### 8.1 Evaluated Configuration

The evaluated version of the TOE consists of Palo Alto Panorama 11.1.9-c2 running on the following physical and virtual appliances (as documented in Section 3.2):

- M-200
- M-300
- M-600
- M-700
- Panorama Virtual Appliance.

The Panorama Virtual Appliance is supported on the following hypervisors:

- VMware ESXi with vSphere 7.0
- Microsoft Hyper-V Server 2019
- Kernel-based Virtual Machine (KVM) on Ubuntu 20.04.

The CCTL conducted evaluation testing of the Panorama Virtual Appliance on the following platforms:

VMware ESXi 7.0:

- Dell PowerEdge R740 Processor: Intel Xeon Gold 6248 (Cascade Lake microarchitecture) with Broadcom 57416 NIC
- Memory: 128 GB RDIMM

Microsoft Hyper-V Server 2019:

- Dell PowerEdge R740 Processor: Intel Xeon Gold 6248 (Cascade Lake microarchitecture) with Broadcom 57416 NIC
- Memory: 128 GB RDIMM

Linux KVM 4 Ubuntu 20.04:

- Dell PowerEdge R740 Processor: Intel Xeon Gold 6248 (Cascade Lake microarchitecture) with Broadcom 57416 NIC
- Memory: 128 GB RDIMM.

In the evaluated configuration, the TOE can be managed by:

- A computer connected to the Management port via an RJ-45 Ethernet cable. The Management port is an out-of-band management port that provides access to the GUI/API via HTTPS or CLI via SSH. The computer is part of the operational environment and requires a web browser (for accessing the GUI) and SSH client (for accessing the CLI).

System logs, which record information about the system such as authentication attempts, session idle timeout, and sessions establishment, termination, failures, are logged and stored locally by default. Configuration logs, which record all management actions, are also logged and stored locally by default.

## 8.2 Excluded Functionality

The table below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. The features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in ST. Only the following protocols implemented by the TOE have been tested, and only to the extent specified by the security functional requirements: TLS, HTTPS, SSH. The features below are out of scope.

Feature	Description
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 are only allowed for pre-operational installation, configuration, and post-operational maintenance and troubleshooting.
API request over HTTP	By default, the TOE supports API requests over HTTPS only. API requests over HTTP are disabled and cannot be enabled in the evaluated configuration.
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.
Any features not associated with SFRs in claimed NDcPP	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities are mentioned in the ST, it is for completeness only.

## 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation team determined the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP/SSHPKG.

### 9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluation team performed the assurance activities specified in the NDcPP/SSHPKG related to the examination of the information contained in the TSS.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in

accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP/SSHPKG and recorded the results in a Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.6 Vulnerability Analysis

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the proprietary Vulnerability Analysis Report prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities.

The evaluation team performed a search of the following public vulnerability databases:

- National Vulnerability Database (<https://nvd.nist.gov/>)
- US-Cert (<https://www.kb.cert.org/vuls/html/search>)
- Tipping Point Zero Day Initiative (<https://www.zerodayinitiative.com/advisories/published/>)
- Palo Alto Networks Security Advisories (<https://security.paloaltonetworks.com/>).

The evaluators performed these searches a number of times, most recently on May 15, 2025.

- The list of software and hardware components that comprise the TOE:
  - Processor:
    - Intel Xeon E5-2620
    - Intel Xeon E5-2680
    - Intel Xeon Silver 4310
    - Intel Xeon Silver 4316
    - Intel Xeon Gold 6248
  - The processors encompass the following microarchitectures:
    - Cascade Lake
    - Broadwell

- Ice Lake
  - Software:
    - Panorama 11.1
    - NGINX (note, the vendor considers the specific version number used within the TOE to be proprietary information—the version number was provided to the evaluation team and used in the search).
  - Virtualization systems on which the Panorama Virtual Appliance is evaluated:
    - ESXi 7.0
    - Hyper-V 2019
    - KVM 4 on Ubuntu 20.04.
- “Palo Alto Networks Crypto Module”, “Palo Alto Panorama”, and “M-200”, “M-300”, “M-600”, and “M-700” as variations of the TOE name.

The evaluation team 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.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

## 10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance documents defined in Section 6 and any additional guidance that it references. No versions of the TOE and software, either earlier or later, were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Specifically, Section 8 defines functionality that was excluded from or not allowed in the evaluated configuration.

Per NIAP Scheme 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.

## 11 Security Target

The ST for this product's evaluation is the *Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 Security Target*, Version 1.0, March 20, 2025.

## 12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCECG	Common Criteria Evaluated Configuration Guide
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DP	Data Plane
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
MP	Management Plane
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PC	Personal Computer
PCL	Product Compliant List
PP	Protection Profile
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report



## 13 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, 00 April 2017
- [5] *collaborative Protection Profile for Network Devices*, Version 3.0e, December 6, 2023
- [6] *Functional Package for Secure Shell (SSH)*, Version 1.0, May 13, 2021
- [7] *Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1 Security Target*, Version 1.0, March 20, 2025
- [8] *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 11.1*, Revision Date: March 20, 2025
- [9] *Panorama Administrator's Guide Version 11.1*, Last Revised August 19, 2024
- [10] *PAN-OS and Panorama API Usage Guide, Version 11.1 & Later*, Last Revised August 21, 2024
- [11] *Assurance Activities Report for Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1*, Version 1.0, May 12, 2025
- [12] *Palo Alto Panorama v11.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 3.0e*, Version 1.0, May 12, 2025
- [13] *Palo Alto Networks Panorama 11.1 Vulnerability Assessment*, Version 1.0, May 15, 2025
- [14] *Palo Alto Networks Flaw Remediation Procedures*, Version 0.1, November 14, 2023
- [15] *Evaluation Technical Report for Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.1*, Version 1.0, May 12, 2025