National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1

Report Number:	**CCEVS-VR-VID11482-2024**
Dated:	**19 September 2024**
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

Acknowledgements

Validation Team

Jim Donndelinger

Jerome Myers

The Aerospace Corporation

Farid Ahmed

Anne Gugel

Robert Wojcik

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Leidos Inc.

Columbia, MD

Contents

1 Executive Summary 4
2 Identification 6
3 TOE Architecture 8
3.1 Hardware Appliances 8
3.2 VM-Series 9
4 Security Policy 10
4.1 Security Audit 10
4.2 Cryptographic Support 10
4.3 User Data Protection 10
4.4 Identification and Authentication 10
4.5 Security Management 10
4.6 Protection of the TSF 11
4.7 TOE Access 11
4.8 Trusted Path/Channels 11
4.9 Stateful Traffic Filtering 11
4.10 Packet Filtering 12
4.11 Intrusion Prevention System 12
5 Assumptions and Clarification of Scope 13
5.1 Assumptions 13
5.2 Clarification of Scope 14
6 Documentation 15
7 IT Product Testing 16
8 TOE Evaluated Configuration 17
9 Results of the Evaluation 20
9.1 Vulnerability Analysis 20
10 Validator Comments/Recommendations 23
11 Security Target 24
12 Abbreviations and Acronyms 25
13 Bibliography 26

List of Tables

Table 1: Evaluation Identifiers 6

Table 2: TOE Security Assurance Requirements 22

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 PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1 (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 TOE was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in September 2024. It 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 documents:

- *Evaluation Activities for Network Device cPP*, Version 3.0e, 6 December 2023 [7]
- *Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module*, Version 1.4 + Errata 20200625, June 2020 [9]
- *Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways*, Version 1.3, 16 August 2023 [11]
- *Supporting Document Mandatory Technical Document, PP-Module for Intrusion Prevention Systems (IPS)*, Version 1.0, 11 May 2021 [13]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [14]

The Leidos evaluation team determined the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 2.0, 25 April 2024 [5] consisting of the following:

- Base PP: collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [6] with the following components
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 [8]
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3, 16 August 2023 [10].
- PP-Module for Intrusion Prevention System (IPS), Version 1.0, 11 May 2021 [12]
- Functional Package for Secure Shell (SSH) Version 1.0, 2021-05-13 [14].

The evaluation further determined that the TOE, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [15]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([22]) and the ST.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the evaluation outputs produced by the evaluation team, in particular 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. 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 (ETR) ([26]) 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 Identifiers

Evaluated Product:	Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1
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:	September 2024
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 3.0e, 6 December 2023 PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 PP-Module for VPN Gateways, Version 1.3, 16 August 2023 PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, 11 May 2021 Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021

Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Anthony Apted Dawn Campbell Justin Fisher Josh Marciante Armin Najafabadi Kofi Owusu Pascal Patin Allen Sant Srilekha Vangala Kevin Zhang
Validation Personnel:	Jerome Myers Jim Donndelinger Farid Ahmed Anne Gugel Robert Wojcik

3 TOE Architecture

3.1 Hardware Appliances

The architecture of the TOE hardware appliances comprises two subsystems: the control plane; and the data plane. The control plane provides system management functionality while the data plane handles all data processing on the network. The TOE can use a non-TOE component—the User Identification Agent, installed on a separate dedicated PC in the operational environment—to retrieve user-specific information that is used for policy enforcement.

The following diagram depicts both the TOE and the User Identification Agent:

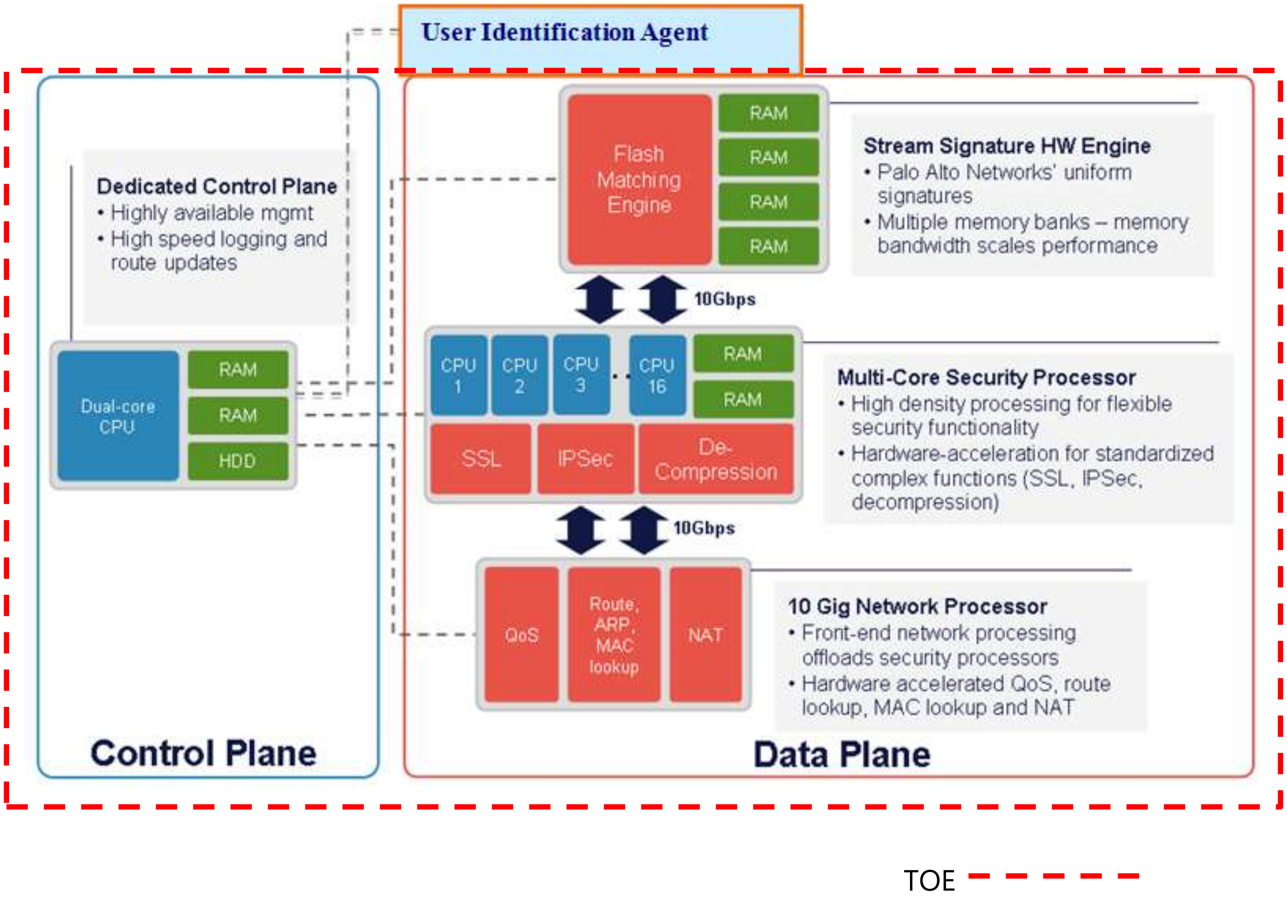
User Identification Agent
Dedicated Control Plane
• Highly available mgmt
• High speed logging and route updates
Dual-core CPU
RAM
RAM
HDD
Control Plane
Flash Matching Engine
RAM
RAM
RAM
RAM
Stream Signature HW Engine
• Palo Alto Networks' uniform signatures
• Multiple memory banks – memory bandwidth scales performance
10Gbps
CPU 1
CPU 2
CPU 3
CPU 16
RAM
RAM
SSL
IPSec
De-Compression
Multi-Core Security Processor
• High density processing for flexible security functionality
• Hardware-acceleration for standardized complex functions (SSL, IPSec, decompression)
10Gbps
QoS
Route, ARP, MAC lookup
NAT
10 Gig Network Processor
• Front-end network processing offloads security processors
• Hardware accelerated QoS, route lookup, MAC lookup and NAT
Data Plane
TOE

Figure 1: TOE Architecture

The control plane includes a multi-core CPU, with dedicated memory and a hard drive for local log, configuration, and software storage. The data plane includes three components—the network processor, the security processor, and the stream signature processor—each with its own dedicated memory and hardware processing.

The control plane provides all device management functionality, including:

- All management interfaces – provide a remote connection for the Web Interface GUI/API and CLI on SSH.
- Configuration management of the device, such as controlling the changes made to the device configuration, as well as the compilation and pushing to the Data Plane of a configuration change.
- Logging infrastructure for traffic, threat, alarm, configuration, and system logs.
- Administration controls, including administrator authentication and audit trail information for administrators logging in, logging out, and configuration changes.
- Interactions with the UIA to retrieve the user to IP address mapping information that is used for policy enforcement (via the Data Plane).

The data plane provides all data processing and security detection and enforcement, including:

- All networking connectivity, packet forwarding, switching, routing, and network address translation.
- Application identification, using the content of the applications, not just port or protocol.
- Application decoding, threat scanning for all types of threats and threat prevention.
- Policy lookups to determine what security policy to enforce and what actions to take, including logging.
- Denial of Service (DoS) protection including TCP Sync flooding attack.
- Logging, with all logs sent to the control plane for processing and storage.

Site-to-site IPsec VPN supports IPv4 or IPv6 site-to-site connections. That is, the administrator can establish IKE and IPsec Security Associations (SAs) between IPv4 or IPv6 endpoints. The web interface can be used to enable, disable, restart, or refresh an IKE gateway or an IPsec VPN tunnel to simplify troubleshooting.

3.2 VM-Series

The VM-Series on specified hardware supports the exact same firewall and threat prevention features that are available in the hardware appliances.

Each VM-Series virtual appliance in its evaluated configuration is installed on a hardware platform, as specified in section 8, that includes a VMware, Linux KVM, or Microsoft Hyper-V hypervisor and an Intel Core or Xeon processor based on the Skylake, Cascade Lake, Ivy Bridge, Haswell, or Broadwell microarchitectures that implement Intel Secure Key, and Network Interface Controllers supported by the server.

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 able to generate audit records of security-relevant events including the events specified in [6], [8], [10], [12], and [14]. 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 and cryptographic hashing and keyed-hash message authentication features in support of higher-level cryptographic protocols, including IPsec, SSH, HTTPS, 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 User Data Protection

The TOE is designed to ensure that it does not inadvertently reuse data found in network traffic.

4.4 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 (HTTPS, SSH, IPsec) connections to the GUI and SSH for interactive administrator sessions and HTTPS for XML and REST API.

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 user and to associate that user with an authorized role. In addition, the TOE can authenticate users using X.509v3 certificates and can be configured to lock a user out after a configurable number of unsuccessful authentication attempts.

4.5 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/API/CLI using an HTTPS/TLS, IPsec, 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 login banner, configure the idle timeout, configure IKE/IPsec VPN gateways, configure threat signature rules, and other management functions. The TOE provides pre-defined Security Administrator, Audit Administrator, and Cryptographic Administrator roles. These administrator roles are all considered Security Administrator as defined in [NDcPP] for the purposes of the evaluation.

4.6 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 and transition to a secure, maintenance state. It also includes a mechanism to verify TOE updates to prevent malicious or other unexpected changes in the TOE.

4.7 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 users the capability to terminate their own interactive sessions.

4.8 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH, HTTP over TLS (HTTPS), or IPsec. SSH, TLS, and IPsec ensure both integrity and disclosure protection. Note: HTTPS traffic can be tunneled through IPsec secure channel.

The TOE uses IPsec or TLS to protect communication with an external log server and protects remote VPN gateways/peers using IPsec to prevent unintended disclosure or modification of the transferred data. The TOE also uses TLS to protect communications with GlobalProtect TLS client applications.

4.9 Stateful Traffic Filtering

The TOE provides a stateful traffic filter firewall for layers 3 and 4 (IP and TCP/UDP) network traffic optimized through the use of stateful packet inspection.

An administrator can configure the TOE to control the type of information that is allowed to pass through the TOE. The administrator defines the security zone and applies security policies to network traffic attempting to traverse the TOE to determine what actions to take.

The TOE groups interfaces into security zones. Each zone identifies one or more interfaces on the TOE. Separate zones must be created for each type of interface (Layer 2, Layer 3, or virtual wire), and each interface must be assigned to a zone before it can process traffic. Security policies provide the firewall rule sets that specify whether to block or allow network connections, based on the source and destination zones, and addresses, and the application service (such as UDP port 67 or TCP port 80). Security policy rules are processed in sequence, applying the first rule that matches the incoming traffic.

4.10 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. An administrator can configure security policies that determine whether to block, allow, or log a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

4.11 Intrusion Prevention System

The TOE provides IPS functionalities such as malicious list blocking, reconnaissance and Denial of Service (DoS) flooding protection, anomaly-based and signature-based traffic detection and response mechanisms.

5 Assumptions and Clarification of Scope

5.1 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 network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
- 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 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. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g., firewall).
- The Security Administrator(s) for the network 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 network 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.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

- 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.
- For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
- For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

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 [7], [9], [11], [13], and [14] 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 PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1 Security Target, Version 1.0, July 8, 2024 [15]. Section 2.4 of [15] 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.

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 Next-Generation Firewall with PAN-OS 11.1, Revision Date: July 9, 2024 [16]
- PAN-OS® Administrator's Guide Version 11.1, Last Revised April 17, 2024 [17]
- PAN-OS CLI Quick Start Version 11.1, Last Revised October 20, 2023 [18]
- PAN-OS Web Interface Help Version 11.1, Last Revised March 13, 2024 [19]
- PAN-OS® and Panorama™ API Usage Guide Version 11.1, Last Revised December 6, 2023 [20]
- VM-Series Deployment Guide Version 11.0, Last Revised November 14, 2022 [21].

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.

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 PAN-OS v11.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 3.0e, Version 1.0, July 11, 2024 [23]

A non-proprietary description of the tests performed is provided in the following document:

- Assurance Activities Report for Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1, Version 1.0, August 15, 2024 [22]

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* [6], *PP-Module for Stateful Traffic Filter Firewalls* [8], *PP-Module for Virtual Private Network (VPN) Gateways* [10], *PP-Module for Intrusion Prevention System (IPS)* [12], and *Functional Package for Secure Shell (SSH)* [14].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Evaluation Activities for Network Device cPP* [7], *Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module* [9], *Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways* [11], *Supporting Document Mandatory Technical Document, PP-Module for Intrusion Prevention Systems (IPS)* [13], and *Functional Package for Secure Shell (SSH)* [14]. 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 from March to July 2024.

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. A description of the test configurations and test tools may be found in section 3.5.1 of the AAR.

- Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the claimed PP and PP-Modules were fulfilled.

8 TOE Evaluated Configuration

The evaluated version of the TOE consists of Palo Alto PAN-OS 11.1.4 running on the following physical and virtual appliances:

- PA-400 Series
  - PA-410
  - PA-410R-5G
  - PA-415
  - PA-415-5G
  - PA-440
  - PA-445
  - PA-450
  - PA-450R
  - PA-450R-5G
  - PA-455
  - PA-460
- PA-800 Series
  - PA-820
  - PA-850
- PA-1400 Series
  - PA-1410
  - PA-1420
- PA-3200 Series
  - PA-3220
  - PA-3250
  - PA-3260
- PA-3400 Series
  - PA-3410
  - PA-3420
  - PA-3430
  - PA-3440
- PA-5200 Series
  - PA-5220
  - PA-5250
  - PA-5260
  - PA-5280[1]
- PA-5400 Series
  - PA-5410
  - PA-5420
  - PA-5430

[1] PA-5280 can operate in Express or Secure mode. Secure mode just means it's 5G-ready and requires a license upgrade.

  - PA-5440
  - PA-5445
- PA-5450[2]
- PA-7000 Series[3]
  - PA-7050
  - PA-7080
  - PA-7500
- VM-Series
  - VM-50
  - VM-100
  - VM-300
  - VM-500
  - VM-700.

The Palo Alto VM-Series is supported on the following hypervisors:

- VMware
  - VMware ESXi with vSphere 7.0
- Linux KVM
  - Ubuntu: 20.04 LTS
- Microsoft Hyper-V Server 2019 ---- The VM-Series firewall can be deployed on a server running Microsoft Hyper-V. Hyper-V is packaged as a standalone hypervisor, called Hyper-V Server 2019, or as an add-on/role for Windows Server 2019.

The CCTL conducted evaluation testing of the VM-Series 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.

Evaluation testing covered the following hardware and processors:

- PA-3260: Cavium Octeon CN7360 MIPS64 (DP) / Intel Pentium D1517 (MP)
- PA-5430: AMD EPYC 7642 (DP/MP)

[2] PA-5450 firewall supports the following cards: PA-5400 MPC-A, PA-5400 NC-A, and PA-5400 DPC-A.

[3] Palo Alto Networks PA-7000 Series firewalls support different Network Processing Cards (NPC) and Switch Management Cards (SMC): PAN-PA-7050-SMC-B, PAN-PA-7080-SMC-B, PAN-PA-7000-LFC-A, PAN-PA-7000-100G-NPC-A-K2-EXP, PAN-PA-7000-100G-NPC-A-K2-SEC, and PAN-PA-7000-100G-NPC.

- PA-5450: Intel Xeon D-2187NT (DP/MP).

The TOE must be deployed as described in section 5.1 of this Validation Report and be configured in accordance with the *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next-Generation Firewall with PAN-OS 11.1* [16].

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.

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 3.0e, December 6, 2023 [7]
- Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 + Errata 20200625, June 2020 [9]
- Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways, Version 1.3, August 16, 2023 [11]
- Supporting Document Mandatory Technical Document, PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, May 11, 2021 [13]
- Functional Package for Secure Shell (SSH) Version 1.0, May 13, 2021 [14].

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 ETR ([26]), which is controlled by the Leidos CCTL. The security assurance requirements are listed in Table 2 below.

9.1 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 [7].

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 several times, most recently on September 17, 2024.

The evaluation team applied the search criteria specified in [7] and [9] as follows:

- The list of software and hardware components that comprise the TOE:
  - Processor:
    - AMD EPYC 7352
    - AMD EPYC 7452
    - AMD EPYC 7642
    - AMD EPYC 7742
    - AMD EPYC 7003
    - Cavium Octeon CN7130
    - Cavium Octeon CN7240
    - Cavium Octeon CN7350
    - Cavium Octeon CN7360
    - Cavium Octeon CN7885
    - Cavium Octeon CN7890
    - Intel Atom C3436L
    - Intel Atom C3558R
    - Intel Atom C3708
    - Intel Atom C3758R
    - Intel Atom C5325
    - Intel Atom C5335C1
    - Intel Atom P5332
    - Intel Atom P5342
    - Intel Atom P5352
    - Intel Atom P5362
    - Intel Atom P5752
    - Intel Pentium D1517
    - Intel Xeon D1548
    - Intel Xeon D1567
    - Intel Xeon D-2187NT
    - Intel D-2798NX
    - Intel Xeon Gold 6248
  - The processors encompass the following microarchitectures:
    - MIPS64
    - Zen 2
    - Zen 3
    - Denverton
    - Tremont
    - Skylake
    - Ice Lake
    - Broadwell

  - Software:
    - PAN-OS 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).

- "Palo Alto Firewall", "Palo Alto Networks Firewall", and "PA-400 Series", "PA-800 Series", "PA-1400 Series", "PA-3200 Series", "PA-3400 Series", "PA-5200 Series", "PA-5400 Series", "PA-5450", and "PA-7000 Series" as variations of the TOE name (and which additionally include the term "firewall")
- Protocols:
  - TCP
  - UDP
  - IPv4
  - IPv6
  - TLS
  - SSH
  - HTTPS
  - IPsec.

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.

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
ALC_FLR.3	Systematic flaw remediation
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope in section 5.2, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Security Target

The ST for this product’s evaluation is Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1 Security Target, Version 1.0, July 8, 2024 [15].

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
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
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
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol
VPN	Virtual Private Network
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] PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 2.0, April 25, 2024

[6] collaborative Protection Profile for Network Devices, Version 3.0e, December 6, 2023

[7] Evaluation Activities for Network Device cPP, Version 3.0e, December 6, 2023

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

[9] Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 + Errata 20200625, June 2020

[10] PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3, August 16, 2023

[11] Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways, Version 1.3, August 16, 2023

[12] PP-Module for Intrusion Prevention System (IPS), Version 1.0, May 11, 2021

[13] Supporting Document Mandatory Technical Document, PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, May 11, 2021

[14] Functional Package for Secure Shell (SSH), Version 1.0, May 13, 2021

[15] Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1 Security Target, Version 1.0, July 8, 2024

[16] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next-Generation Firewall with PAN-OS 11.1, Revision Date: July 9, 2024

[17] PAN-OS® Administrator's Guide Version 11.1, Last Revised April 17, 2024

[18] PAN-OS CLI Quick Start Version 11.1, Last Revised October 20, 2023

[19] PAN-OS Web Interface Help Version 11.1, Last Revised March 13, 2024

[20] PAN-OS® and Panorama™ API Usage Guide Version 11.1, Last Revised December 6, 2023

[21] VM-Series Deployment Guide Version 11.0, Last Revised November 14, 2022.

[22] Assurance Activities Report for Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1, Version 1.0, September 18, 2024.

[23] Palo Alto PAN-OS v11.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 3.0e, Version 1.0, July 11, 2024.

[24] Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1 Vulnerability Assessment, Version 1.2, September 17, 2024.

[25] Palo Alto Networks Flaw Remediation Procedures, Version 0.1, November 14, 2023.

[26] Evaluation Technical Report for Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.1, Version 1.0, September 18, 2024.