National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1

Report Number:	**CCEVS-VR-VID11284-2022**
Dated:	**August 31, 2022**
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

Meredith Martinez

Seada Mohammed

Jerome Myers

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, 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-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 (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

PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 (PAN-OS Firewalls) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2022.

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 documents:

- Evaluation Activities for Network Device cPP, Version 2.2, December 2019 [6]
- Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 + Errata 20200625, June 2020 [8]
- Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways, Version 1.2, 31 March 2022 [10]

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 function as a stateful traffic filter firewall and VPN gateway. The focus of the evaluation was on the product's conformance to the security functionality specified in the following documents:

- PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 [20]
- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [5]
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 [7]
- PP-Module for VPN Gateways, Version 1.2, 31 March 2022 [9]

The security functions specified in this Protection Profile (PP) and PP-Modules include protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and enforcement of network traffic filtering rules.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and PP-Modules and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [11]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([19]) and the associated test report produced by the Leidos evaluation team ([18]).

The validation team 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. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6], [8], and [10] 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.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0527 – Updates to Certificate Revocation Testing (FIA_X509_EXT.1)
- TD0536 – NIT Technical Decision for Update Verification Inconsistency
- TD0537 – NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3
- TD0538 – NIT Technical Decision for Outdated link to allowed-with list
- TD0545: NIT Technical Decision for Conflicting FW rules cannot be configured (extension of Rfl#201837)
- TD0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN
- TD0551: NIT Technical Decision for Incomplete Mappings of OEs in FW Module v1.4+Errata
- TD0555 – NIT Technical Decision for RFC Reference incorrect in TLSS Test
- TD0556 – NIT Technical Decision for RFC 5077 question
- TD0563 – NIT Technical Decision for Clarification of audit date information
- TD0564 – NIT Technical Decision for Vulnerability Analysis Search Criteria
- TD0569 – NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7
- TD0570 – NIT Technical Decision for Clarification about FIA_AFL.1
- TD0571 – NIT Technical Decision for Guidance on how to handle FIA_AFL.1
- TD0572 – NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers
- TD0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e
- TD0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3

- TD0591 – NIT Technical Decision for Virtual TOEs and hypervisors
- TD0592 – NIT Technical Decision for Local Storage of Audit Records
- TD0631 – NIT Technical Decision for Clarification of Public Key Authentication for SSH Server
- TD0632 – NIT Technical Decision for Consistency with Time Data for vNDs
- TD0633 – NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance
- TD0634 – NIT Technical Decision for Clarification Required for Testing IPv6
- TD0635 – NIT Technical Decision for TLS Server and Key Agreement Parameters
- TD0657 – IPSEC_EXT.1.6 GCM support for VPN GW

All other Technical Decisions were found to be not applicable to the TOE, either because they were not related to the claimed Protection Profile and PP-Modules or because they related to optional or selection-based functionality that was not claimed in the TOE's Security Target [7].

1.2 Threats

The ST references the PP and PP-Modules to which it claims conformance for statements of threats that the TOE and its operational environment are intended to counter. Those threats, drawn from the claimed PP and PP-Modules, are as follows:

From collaborative Protection Profile for Network Devices:

- Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man in the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
- Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
- Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated

using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

- Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
- Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
- Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.
- An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

From PP-Module for Stateful Traffic Filter Firewalls:

- An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
- With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.
- An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.
- An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

From PP-Module for VPN Gateways:

- Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices, then the data contained within the communications may be susceptible to a loss of integrity.
- Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network
- Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on

the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.

- Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.
- If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver.

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 PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1
Security Target:	Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 Security Target, Version 1.1, 31 August 2022
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 31, 2022
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 2.2e, 23 March 2020 PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 PP-Module for VPN Gateways, Version 1.2, 31 March 2022
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE

Evaluation Personnel:

Tony Apted
Greg Beaver
Justin Fisher
Josh Marciante
Kofi Owusu
Pascal Patin
Allen Sant

Validation Personnel:

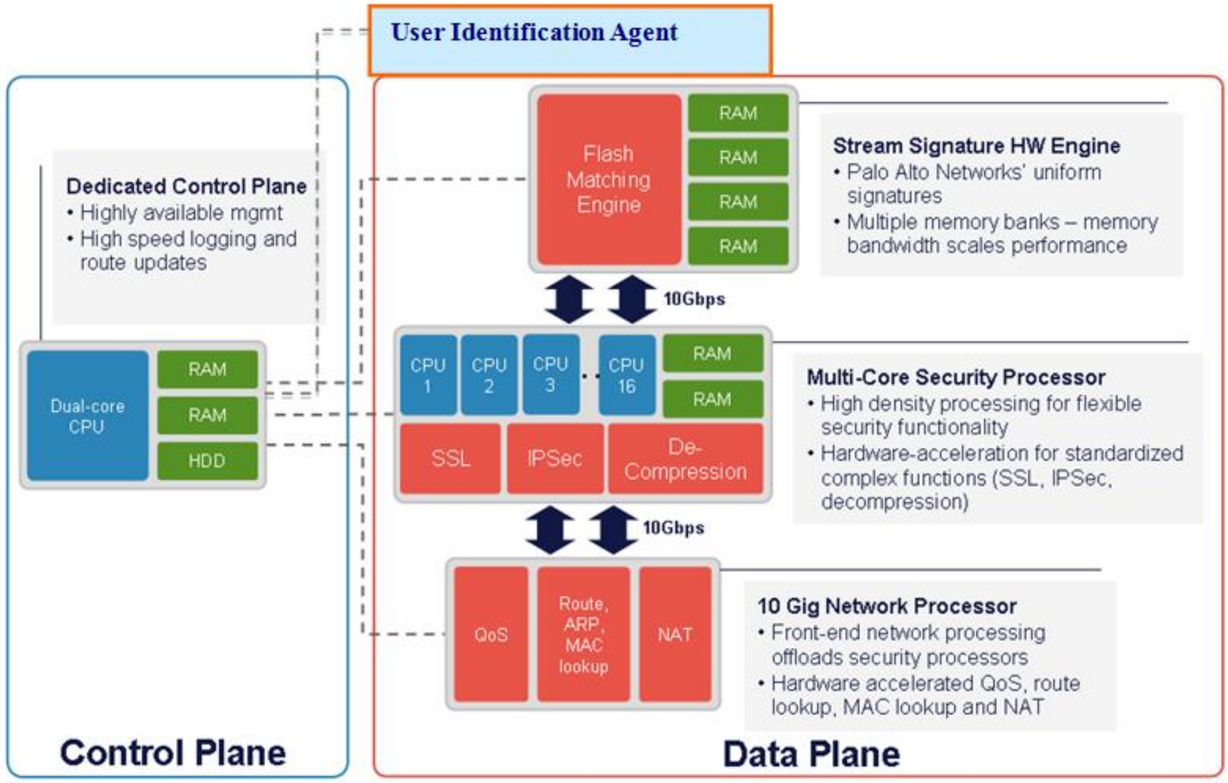
Meredith Martinez
Seada Mohammed
Jerome Myers

3 TOE Architecture

The firewalls' architecture is divided into 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; both reside on the firewall appliance. The TOE relies on the User Identification Agent installed on a separate dedicated PC in the operational environment to retrieve user-specific information that is uses for policy enforcement.

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

Figure 1: TOE Architecture


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

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.

In summary, the functionality provided by each component of the system is as follows:

Control Plane (also known as Management Plane)

The control plane provides all device management functionality, including:

- All management interfaces – provide a both direct and 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).

Data Plane (DP)

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, you 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.

VM-Series

The VM-Series on specified hardware supports the exact same next-generation firewall and advanced threat prevention features that are available in the physical form factor appliances, allowing an administrator to safely enable applications flowing into, and across private, public and hybrid cloud computing environments.

Each VM-Series virtual appliance in its evaluated configuration is installed on a hardware platform as specified in Section 1.1 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.

3.1 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.
- Virtualized Firewalls installed on specified hardware - the VM-Series supports the exact same next-generation firewall and advanced threat prevention features available in the physical form factor appliances, allowing an administrator to safely enable applications flowing into, and across your private, public and hybrid cloud 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 PAN-OS VMs. VMs are deployed in the system using Intel CPUs.

- PAN-OS v10.1 – the software/firmware component that runs the appliance. For VMs PAN-OS is software and for hardware appliances PAN-OS is firmware. PAN-OS is built on top of a Linux kernel and runs along with NGINX (the web server that Palo Alto Networks uses), crond, syslogd, and various vendor-developed applications that implement PAN-OS capabilities. PAN-OS provides the logical interfaces for network traffic. PAN-OS runs on both the Control Plane and the Data Plane and provides all firewall functionalities provided by the TOE, including the threat prevention capabilities as well as the identification and authentication of users and the management functions. PAN-OS provides unique functionality on the two planes based on the applications that are executing. The Control Plane provides a GUI Web management interface to access and manage the TOE functions and data. The Data Plane provides the external interface between the TOE and the external network to monitor network traffic so that the TSF can enforce the TSF security policy.

The physical boundary of the TOE comprises the firewall appliance (PA-220, PA-220R, PA-410, PA-440, PA-450, PA-460, PA-820, PA-850, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-5450, PA-7050, and PA-7080); and the virtual appliances on specified hardware in the VM-Series VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV. The next-generation firewall models differ in their performance capability, but they provide the same security functionality.

Virtual systems are supported by default (without an additional license) on the PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-5450, PA-7050, and PA-7080. The PA-220 and PA-800 cannot support virtual systems. Virtual systems specify a collection of physical and logical firewall interfaces that should be isolated. Each virtual system contains its own security policy and its own set of logs that will be kept separate from all other virtual systems.

The firewall appliance attaches to a physical network and includes the following ports and processors:

- PA-220: 8 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port); 1 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and DC Power input. Processor: Cavium Octeon CN7130 MIPS64 (DP/MP)
- PA-220R: 6 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port), 1 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and DC Power input. Processor: Cavium Octeon CN7130 MIPS64 (DP/MP)
- PA-410: 7 RJ-45 10/100/100 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port); 2 USB (disabled in FIPS-CC mode except for power) and Power input. Processor: Intel Atom C3634L (DP/MP)
- PA-440/PA-450/PA-460: 8 RJ-45 10/100/100 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port); 2 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and Power input. Processor: Intel Atom C3558R (DP/MP) for 440 and Intel Atom C3758R (DP/MP) for 450 and 460.
- PA-820: 4 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 8 Small Form-Factor Pluggable (SFP) Gbps ports for network traffic; 1 RJ-45 port to access the device GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console

(management console port); 1 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and 100-240V Power input. Processor: Cavium Octeon CN7240 MIPS64 (DP/MP)

- PA-850: 4 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 4/8 SFP; 0/4 SFP+ connectors for network traffic; 1 RJ-45 port to access the device GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port); 1 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and 100-240V Power input. Processor: Cavium Octeon CN7240 MIPS64 (DP/MP)
- PA-3220/PA-3250: 12 RJ-45 10/100/1000 ports for network traffic. 8 Small Form-Factor Pluggable (SFP) ports for network traffic. 1 RJ-45 port to access the device management interfaces through an Ethernet interface. 1 RJ-45 port for connecting a serial console. 2 RJ-45 ports for high-availability (HA) control and synchronization, 1 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and 2 Power inputs. Processor: Cavium Octeon CN7350 MIPS64 (DP) / Intel Pentium D1517 (MP)
- PA-3260: 12 RJ-45 10/100/1000 ports for network traffic. 8 Small Form-Factor Pluggable (SFP) ports for network traffic. 1 RJ-45 port to access the device management interfaces through an Ethernet interface. 1 RJ-45 port for connecting a serial console. 2 RJ-45 ports for high-availability (HA) control and synchronization , 1 USB (disabled in FIPS-CC mode except for power), 1 Micro USB Console (self-test output only in FIPS-CC mode), and 2 Power inputs. Processor: Cavium Octeon CN7360 MIPS64 (DP) / Intel Pentium D1517 (MP)
- PA-5220: 4 100/1000/10G Cu, 16 1G/10G SFP/SFP+, 4 40G QSFP+ for network traffic; 2 RJ-45 port to access the device management interfaces through an Ethernet interface; 1 RJ-45 port for connecting a serial console, 1 40G QSFP+ HA for high-availability (HA) control and synchronization, 1 USB (disabled in FIPS-CC mode except for power), and 2 100-240V Power inputs. Processor: Cavium Octeon CN7885 MIPS64 (DP) / Intel Xeon D1548 (MP)
- PA-5250: 4 100/1000/10G Cu, 16 1G/10G SFP/SFP+, 4 40G/100G QSFP28 for network traffic; 2 RJ-45 port to access the device management interfaces through an Ethernet interface; 1 RJ-45 port for connecting a serial console, 1 40G/100G QSFP28 for high-availability (HA) control and synchronization, 1 USB (disabled in FIPS-CC mode except for power), and 2 100-240V Power inputs. Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Xeon D1567 (MP)
- PA-5260/PA-5280: 4 100/1000/10G Cu, 16 1G/10G SFP/SFP+, 4 40G/100G QSFP28 for network traffic; 2 RJ-45 port to access the device management interfaces through an Ethernet interface; 1 RJ-45 port for connecting a serial console, 1 40G/100G QSFP28 for high-availability (HA) control and synchronization, 1 USB (disabled in FIPS-CC mode except for power), and 2 100-240V Power inputs. Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Xeon D1567 (MP)
- PA-5450: For network connectivity, the PA-5450 requires at least one NC (PA-5400-NC-A). Each PA-5400-NC-A offers multiple connectivity ports as listed: 100/1000/10G Cu (4), 1G/10G SFP/SFP+ (12), and 40G/100G QSFP28 (2), and 2 Power inputs. For packet and security processing, the PA-5450 uses DPCs (PA-5400-DPC-A). The MPC (PAN-PA-5400-MPC-A) acts as a dedicated point of contact for controlling all aspects of the PA-5450 and has 2 HA ports, 1 RJ-45 Console port, 2 Management ports, 1 USB (disabled in FIPS-CC mode except for power) and 1 Micro USB Console (self-test output only in FIPS-CC mode). Processor: Intel Xeon D-2187NT (DP/MP)

- PA-7050: 12 gig copper ports for network traffic, 8 Small Form-Factor Pluggable (SFP) ports for network traffic and 4 SFP+ ports for network traffic per blade OR 2 Quad Small Form-Factor Pluggable (QSFP) for network traffic per blade and 12 SFP+ ports for network traffic per blade (6 blades max). 1 RJ-45 port to access the device management interfaces through an Ethernet interface. 1 RJ-45 port for connecting a serial console. 2 QSFP ports for high-availability (HA) control and synchronization, 1 USB (disabled in FIPS-CC mode except for power), and 4 100-240V Power inputs. Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Core i7-2715QE (MP)
- PA-7080: 12 gig copper ports for network traffic, 8 Small Form-Factor Pluggable (SFP) ports for network traffic and 4 SFP+ ports for network traffic per blade OR 2 Quad Small Form-Factor Pluggable (QSFP) for network traffic per blade and 12 SFP+ ports for network traffic per blade (10 blades max). 1 RJ-45 port to access the device management interfaces through an Ethernet interface. 1 RJ-45 port for connecting a serial console. 2 QSFP ports for high-availability (HA) control and synchronization, 1 USB (disabled in FIPS-CC mode except for power), and 8 100-240V Power inputs. Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Core i7-2715QE (MP)

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

- A computer either directly connected or remotely 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 required to have a web browser (for accessing the GUI) and SSH client (for accessing the CLI).

Traffic logs, which record information about each traffic flow or problems with the network traffic, are logged locally by default. However, the product offers the capability to send the logs as SNMP traps, Syslog messages, or email notifications. Traffic logging and the use of email notifications and the SNMP and SMTP servers have not been subject to testing in the evaluated configuration.

The operational environment includes the following:

- Syslog server
- VPN gateway peer(s)
- Palo Alto Networks GlobalProtect application
- Workstation
  - Web browsers - Chrome (version 96 or later), Firefox (version 94.0.2 or later), Safari (version 12.0.3 or later on Mac, and version 5.1.7 or later on Windows and iOS), and Microsoft Edge (Release 42 or later) browser.
  - SSHv2 client

The operational environment includes a domain controller and the User Identification Agent is installed on one or more PCs in the operational environment, and is supported on Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

Table 2: TOE Platforms

Product Identification	Illustration	Description
PA-220		• 500 Mbps firewall throughput (App-ID enabled • 150 Mbps threat prevention throughput • 100 Mbps IPsec VPN throughput • 64,000 max sessions • 4,200 new sessions per second • 250 IPsec VPN tunnels/tunnel interfaces • 15 security zones • 250 max number of policies
PA-220R		• 500/560 Mbps firewall throughput (App-ID enabled • 150/260 Mbps threat prevention throughput • 100 Mbps IPsec VPN throughput • 64,000 max sessions • 4,200 new sessions per second • 250 IPsec VPN tunnels/tunnel interfaces • 15 security zones • 250 max number of policies
PA-410		• 1.7/1.3 Gbps Firewall throughput (HTTP/appmix) • 0.6/0.7 Gbps Threat Prevention throughput (HTTP/appmix) • 0.93 Gbps IPsec VPN throughput • 64,000 max sessions • 13,000 New sessions per second
PA-440		• 3.0/2.4 Gbps Firewall throughput (HTTP/appmix) • 0.9/1.0 Gbps Threat Prevention throughput (HTTP/appmix) • 1.6 Gbps IPsec VPN throughput • 200,000 max sessions • 39,000 New sessions per second
PA-450		• 3.8/3.2 Gbps Firewall throughput (HTTP/appmix) • 1.6/1.7 Gbps Threat Prevention throughput (HTTP/appmix) • 2.2 Gbps IPsec VPN throughput • 300,000 max sessions

Product Identification	Illustration	Description
		• 52,000 New sessions per second
PA-460		• 5.2/4.7 Gbps Firewall throughput (HTTP/appmix) • 2.4/2.6 Gbps Threat Prevention throughput (HTTP/appmix) • 3.1 Gbps IPsec VPN throughput • 400,000 max sessions • 74,000 New sessions per second
PA-820		• 1.9 Gbps firewall throughput (App-ID enabled) • 780 Mbps threat prevention throughput • 500 Mbps IPsec VPN throughput • 192,000 max sessions • 9,500 new sessions per second • 1000 IPsec VPN tunnels/tunnel interfaces • 5 virtual routers • 40 security zones • 1,500 max number of policies
PA-850		• 1.9 Gbps firewall throughput (App-ID enabled) • 780 Mbps threat prevention throughput • 500 Mbps IPsec VPN throughput • 192,000 max sessions • 9,500 new sessions per second • 1000 IPsec VPN tunnels/tunnel interfaces • 5 virtual routers • 40 security zones • 1,500 max number of policies
PA-3220		• 4.6/4.6 Gbps firewall throughput (App-ID enabled) • 2.2/2.6 Gbps Threat Prevention throughput • 2.5 Gbps IPsec VPN throughput • 1,000,000 max sessions • 57,000 new sessions per second • 4,000 IPsec VPN tunnels/tunnel interfaces • 1,024 SSL VPN Users • 10 virtual routers • 1/6 virtual systems (base/max) • 200 security zones • 2,500 max number of policies

Product Identification	Illustration	Description
PA-3250		- 6/7 Gbps firewall throughput (App-ID enabled) - 2.6/3.1 Gbps Threat Prevention throughput - 3.2 Gbps IPsec VPN throughput - 2,000,000 max sessions - 84,000 new sessions per second - 6,000 IPsec VPN tunnels/tunnel interfaces - 2,048 SSL VPN Users - 10 virtual routers - 1/6 virtual systems (base/max) - 200 security zones - 5,000 max number of policies
PA-3260		- 8.4/10 Gbps firewall throughput (App-ID enabled) - 3.9/4.7 Gbps Threat Prevention throughput - 4.8 Gbps IPsec VPN throughput - 3,000,000 max sessions - 118,000 new sessions per second - 6,000 IPsec VPN tunnels/tunnel interfaces - 2,048 SSL VPN Users - 10 virtual routers - 1/6 virtual systems (base/max) - 200 security zones - 5,000 max number of policies
PA-5220		- 17/20 Gbps firewall throughput (HTTP/appmix) - 8/9 Gbps Threat Prevention throughput (HTTP/appmix) - 8 Gbps IPsec VPN throughput - 4,000,000 max sessions - 150,000 New sessions per second - 20 virtual routers - 10/20 Virtual systems (base/max)
PA-5250		- 39/40 Gbps firewall throughput (HTTP/appmix) - 18/23 Gbps Threat Prevention throughput (HTTP/appmix) - 16 Gbps IPsec VPN throughput - 8,000,000 max sessions

Product Identification	Illustration	Description
		• 284,000 New sessions per second • 125 virtual routers • 25/125 Virtual systems (base/max)
PA-5260		• 60/67 Gbps Firewall throughput (HTTP/appmix) • 28/33 Gbps Threat Prevention throughput (HTTP/appmix) • 24 Gbps IPsec VPN throughput • 32,000,000 max sessions • 390,000 New sessions per second • 225 virtual routers • 25/225 Virtual systems (base/max)
PA-5280		• 60/67 Gbps Firewall throughput (HTTP/appmix) • 28/33 Gbps Threat Prevention throughput (HTTP/appmix) • 24 Gbps IPsec VPN throughput • 64,000,000 max sessions • 390,000 New sessions per second • 225 virtual routers • 25/225 Virtual systems (base/max)
PA-5450		• 200/200 Gbps Firewall throughput (HTTP/appmix) • 120/148 Gbps Threat Prevention throughput (HTTP/appmix) • 79 Gbps IPsec VPN throughput • 100,000,000 max sessions • 3.5M New sessions per second • 25/225 Virtual systems (base/max)
PA-7050		• 380/430 Gbps firewall throughput • 366 Gbps Threat Prevention throughput (DSRI enabled) • 176/210 Gbps Threat Prevention throughput • 144 Gbps IPsec VPN throughput

Product Identification	Illustration	Description
		• 192 M max sessions • 2.9 M new sessions per second • 25/225 virtual systems (base/max)
PA-7080		• 630/720 Gbps firewall throughput • 610 Gbps Threat Prevention throughput (DSRI enabled) • 294/350 Gbps Threat Prevention throughput • 240 Gbps IPsec VPN throughput • 320 M max sessions • 4.8 M new sessions per second • 25/225 virtual systems (base/max)
Virtual Appliances		
VM-50		• 50,000 max sessions • 250 security rules • 1,000 dynamic IP addresses • 15 Security zones • 250 IPsec VPN tunnels • 250 TLS VPN tunnels
VM-100		• 250,000 max sessions • 1,500 security rules • 2,500 dynamic IP addresses • 40 Security zones • 1,000 IPsec VPN tunnels • 500 TLS VPN tunnels
VM-200		• 250,000 max sessions • 1,500 security rules • 2,500 dynamic IP addresses • 40 Security zones • 1,000 IPsec VPN tunnels • 500 TLS VPN tunnels
VM-300		• 800,000 max sessions • 10,000 security rules • 100,000 dynamic IP addresses • 40 Security zones • 2,000 IPsec VPN tunnels • 2,000 TLS VPN tunnels

Product Identification	Illustration	Description
VM-500		- 2,000,000 max sessions - 10,000 security rules - 100,000 dynamic IP addresses - 200 Security zones - 4,000 IPsec VPN tunnels - 6,000 TLS VPN tunnels
VM-700		- 10, 000,000 max sessions - 20,000 security rules - 100000 dynamic IP addresses - 200 Security zones - 8,000 IPsec VPN tunnels - 12,000 TLS VPN tunnels
VM-1000-HV		- 800,000 max sessions - 10,000 security rules - 100,000 dynamic IP addresses - 40 Security zones - 2,000 IPsec VPN tunnels - 2,000 TLS VPN tunnels

3.2 Logical Boundaries

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 Evaluation Technical Report (ETR).

3.2.1 Security Audit

The TOE is able to generate audit records of security-relevant events including the events specified in the claimed PP and PP-Modules. 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.

3.2.2 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.

3.2.3 User Data Protection

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

3.2.4 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) and direct 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.

3.2.5 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 locally via direct RJ-45 Ethernet cable connection and remotely 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, 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 the claimed PP for the purposes of the evaluation.

3.2.6 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.

3.2.7 TOE Access

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

3.2.8 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 protects communication with the Global Protect application using TLS connections; the external log server with IPsec or TLS; and remote VPN gateways/peers using IPsec to prevent unintended disclosure or modification of the transferred data.

3.2.9 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.

3.2.10 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 Assumptions and Clarification of Scope

4.1 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 device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will 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.
- The device is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent of the functionality that is evaluated for conformance to the NDcPP is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. 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 Certificate Authority (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 are 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.
- 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.

4.2 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 PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 Security Target, Version 1.1, August 31, 2022 [11]. Section 2.4 of [11] 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.

5 TOE Evaluated Configuration

5.1 Evaluated Configuration

The TOE is the Palo Alto Networks

PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report. The specific appliance models include:

1. PA-220 Series
    a. PA-220
    b. PA-220R
2. PA-400 Series
    a. PA-410
    b. PA-440
    c. PA-450
    d. PA-460
3. PA-800 Series
    a. PA-820
    b. PA-850
4. PA-3200 Series
    a. PA-3220
    b. PA-3250
    c. PA-3260
5. PA-5200 Series
    a. PA-5220
    b. PA-5250
    c. PA-5260
    d. PA-5280[1]
6. PA-5450[2]
7. PA-7000 Series[3]

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

[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-7050-SMC, PAN-PA-7080-SMC, PAN-PA-7000-100G-NPC-A-K2-EXP, PAN-PA-7000-100G-NPC-A-K2-SEC, PAN-PA-7000-20GXM-NPC, PAN-PA-7000-20GQXM-NPC, and PAN-PA-7000-100G-NPC.

   a. PA-7050
   b. PA-7080

8. VM-Series
   a. VM-50
   b. VM-100
   c. VM-200
   d. VM-300
   e. VM-500
   f. VM-700
   g. VM-1000-HV

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

- VMware
  - VMware ESXi with vSphere 7.0
- Linux KVM
  - Ubuntu: 18.04 LTS
  - Ubuntu: 20.04 LTS
- Microsoft Hyper-V Server 2012 R2, Server 2016, or 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 TOE includes a “FIPS-CC” mode of operation. This mode must be enabled for the TOE to meet the claimed requirements.

5.2 Excluded Functionality

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

- Telnet and HTTP Management Protocols: Telnet and HTTP are disabled by default and cannot be enabled in the evaluated configuration. Telnet and HTTP are insecure protocols which allow for plaintext passwords to be transmitted. Use SSH and HTTPS only as the management protocols to manage the TOE.
- External Authentication Servers: The NDcPP does not require external authentication servers.
- Shell and Console Access: The shell and console access is only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting.
- TLS and SSH Decryption Policies: This functionality is outside the scope of the claimed PP and PP-Modules.
- Anti-Virus, Anti-Spyware, Anti-Malware Security Policies: This functionality is outside the scope of the claimed PP and PP-Modules.
- File Blocking, DLP, and URL Filtering Security Policies: This functionality is outside the scope of the claimed PP and PP-Modules.

- API request over HTTP: By default, the TOE support API requests over HTTPS only. API request over HTTP is disabled and cannot be enabled in the evaluated configuration.
- Any features not associated with SFRs defined in the claimed PP or PP-Modules: Exact conformance requires the TOE not to claim functionality that is not defined in a PP or PP-Module to which it claims conformance.
- Non- FIPS-CC mode of operation.

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 Firewalls with PAN-OS 10.1, August 31, 2022 [12]
- PAN-OS® Administrator's Guide Version 10.1, Last Revised April 8, 2022 [13]
- VM-Series Deployment Guide Version 10.1, Last Revised December 17, 2021 [14]
- PAN-OS CLI Quick Start Version 10.1, Last Revised May 27, 2021 [15]
- PAN-OS Web Interface Help Version 10.1, Last Revised July 25, 2022 [16]
- PAN-OS and Panorama API Usage Guide Version 10.1, Last Revised March 15, 2022 [17].

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

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

7 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 PanOS v10.1 Common Criteria Test Report and Procedures, Version 1.1, August 31, 2022 [18]

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 Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1, Version 1.1, August 31, 2022 [19]

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], *PP-Module for Stateful Traffic Filter Firewalls* [7], and *PP-Module for VPN Gateways* [9].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *collaborative Protection Profile for Network Devices* [5], *PP-Module for Stateful Traffic Filter Firewalls* [7], and *PP-Module for VPN Gateways* [9]. 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 the claimed PP and PP-Modules were fulfilled.

7.1 Test Configuration

The evaluated version of the TOE consists of Palo Alto PAN-OS 10.1.6-h4 running on any of the following physical and virtual appliances:

1. PA-220 Series
    a. PA-220
    b. PA-220R
2. PA-400 Series
    a. PA-410
    b. PA-440
    c. PA-450
    d. PA-460
3. PA-800 Series
    a. PA-820

   b. PA-850

4. PA-3200 Series
   a. PA-3220
   b. PA-3250
   c. PA-3260
5. PA-5200 Series
   a. PA-5220
   b. PA-5250
   c. PA-5260
   d. PA-5280[4]
6. PA-5450[5]
7. PA-7000 Series[6]
   a. PA-7050
   b. PA-7080
8. VM-Series
   a. VM-50
   b. VM-100
   c. VM-200
   d. VM-300
   e. VM-500
   f. VM-700
   g. VM-1000-HV

The TOE must be deployed as described in section **Error! Reference source not found.**.1 of this Validation Report and be configured in accordance with the *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next-Generation Firewalls with PAN-OS 10.1* [12].

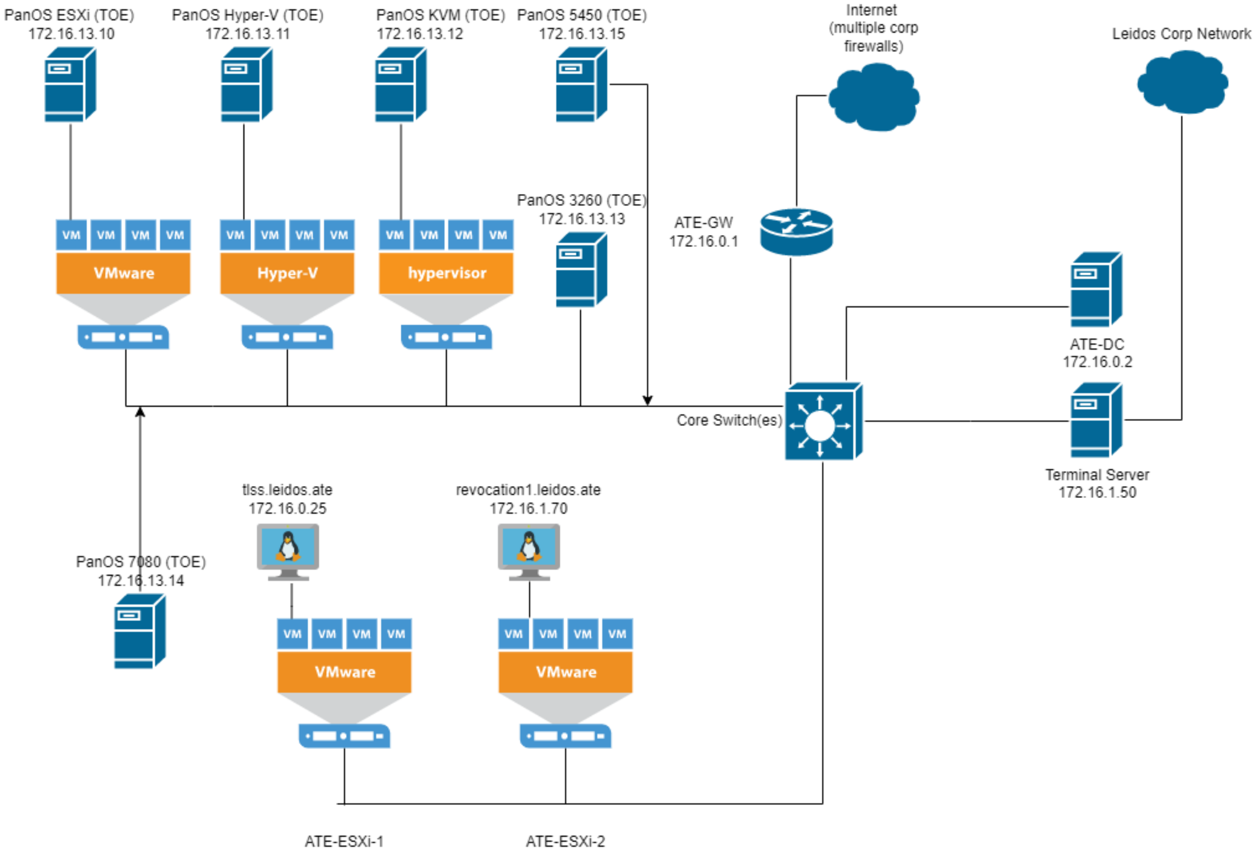
Figure 1 below is a diagram of the test environment configuration, and the list of test tool and versions can be found in the AAR, Section 3.5.

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

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

[6] 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-7050-SMC, PAN-PA-7080-SMC, PAN-PA-7000-100G-NPC-A-K2-EXP, PAN-PA-7000-100G-NPC-A-K2-SEC, PAN-PA-7000-20GXM-NPC, PAN-PA-7000-20GQXM-NPC, and PAN-PA-7000-100G-NPC.

Figure 2: TOE Test Configuration Diagram



7.2 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 August 4, 2022.

The evaluation team applied the search criteria specified in [6] and [8] as follows:

- The list of software and hardware components that compose the TOE:
  - Processor:
    - Cavium Octeon CN7130
    - Cavium Octeon CN7240
    - Cavium Octeon CN7350
    - Cavium Octeon CN7360
    - Cavium Octeon CN7885
    - Cavium Octeon CN7890
    - Intel Atom C3634L
    - Intel Atom C3558R

        - Intel Atom C3758R
        - Intel Pentium D1517
        - Intel Xeon D1548
        - Intel Xeon D1567
        - Intel Xeon D-2187NT
        - Intel Core i7-2715
        - Intel Xeon Gold 6248
    - The processors consist of the following microarchitectures
        - MIPS64
        - Skylake
        - Cascade Lake
        - Ivy Bridge
        - Haswell
        - Broadwell
    - Software:
        - PAN-OS 10.1.6

- “Palo Alto Firewall”, “Palo Alto Networks Firewall”, and “PA-220 Series”, “PA-400 Series”, “PA-800 Series”, “PA-3200 Series”, “PA-5200 Series”, “PA-5450”, and “PA-7000 Series” as variations of the TOE name (and which additionally include the term “firewall”)
- Protocols, restricted to vulnerabilities published after 6/25/2020—since these protocols are pervasive in IT products, there is little value in attempting to search vulnerability repositories such as the NVD using just the protocol (e.g., “TCP”). Such a search produces thousands of results, the vast majority of which are specific to a particular product that is unrelated to the TOE. Therefore, when searching public vulnerability repositories, the evaluation team includes the vendor name.
    - 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.

8 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 2.2, December 2019 [6]
- Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 + Errata 20200625, June 2020 [8]
- Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways, Version 1.2, 31 March 2022 [10]

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.

8.1 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 TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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.

8.2 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 Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the PP related to the examination of the information contained in the TSS.

The validator 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.

8.3 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 validator 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.

8.4 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 validator 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.

8.5 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 PP and recorded the results in a Test Report, summarized in the Assurance Activities Report (AAR).

The validator 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.

8.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The evaluation team performed a search of publicly available information to identify potential vulnerabilities in the TOE using guidelines from Labgram #116/Valgram #135.

Please see Section 7.2 for details on the vulnerability analysis performed by evaluation team.

The validator 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.

8.7 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.

9 Validator Comments/Recommendations

It should be noted: Before you can begin using the TOE for application-level filtering, VPN, and IPS/IDS, you are required to register, activate, and retrieve the device support and licenses. Every instance of firewall requires valid licenses that entitle you to use the firewalls and obtain support. This license is based on firewall serial numbers, not on the number of virtual systems on each firewall. The support license enables the TOE software updates and dynamic content updates (for the latest Applications and Threats signatures, as an example).

All other validator comments are addressed in Section 4, Assumptions and Clarification of Scope.

10 Annexes

Not applicable

11 Security Target

The ST for this product's evaluation is *Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1 Security Target, Version 1.1, August 31, 2022* [11].

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
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
DLP	Data Loss Prevention
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
KVM	Kernel-based Virtual Machine
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
PIN	Personal Identification Number
PP	Protection Profile
REST	Representational State Transfer
SSH	Secure Socket Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network
VR	Validation Report
XML	Extensible Markup Language

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 2.2e, 23 March 2020

[6] Evaluation Activities for Network Device cPP, Version 2.2, December 2019

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

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

[9] PP-Module for VPN Gateways, Version 1.2, 31 March 2022

[10] Supporting Document Mandatory Technical Document, PP-Module for VPN Gateways, Version 1.2, 31 March 2022

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

[12] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next-Generation Firewalls with PAN-OS 10.1, August 31, 2022

[13] PAN-OS® Administrator’s Guide Version 10.1, Last Revised April 8, 2022

[14] VM-Series Deployment Guide Version 10.1, Last Revised December 17, 2021

[15] PAN-OS CLI Quick Start Version 10.1, Last Revised May 27, 2021

[16] PAN-OS Web Interface Help Version 10.1, Last Revised July 25, 2022

[17] PAN-OS and Panorama API Usage Guide Version 10.1, Last Revised March 15, 2022

[18] Palo Alto PanOS v10.1 Common Criteria Test Report and Procedures, Version 1.1, August 31, 2022

[19] Assurance Activities Report for Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1, Version 1.1, August 31, 2022

[20] PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022

[21] Evaluation Technical Report For Palo Alto Networks PA-220 Series, PA-400 Series, PA-800 Series, PA-3200 Series, PA-5200 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 10.1, Version 1.1, August 31, 2022