National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

for

Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0

Report Number: CCEVS-VR-VID11063-2020
Dated: 14 October 2020
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Jerome Myers, PhD

Marybeth Panock

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Anthony Apted

Dawn Campbell

Kevin Steiner

Pascal Patin

Justin Fisher

Punit Patel

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report 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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in October 2020. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the product is:

- Common Criteria Part 2 Extended and Part 3 Conformant,

and

- demonstrates exact conformance to the
    - collaborative Protection Profile for Network Devices, Version 2.1, September 2018
    - PP-Module for Stateful Traffic Filter Firewalls Version 1.3 27-September-2019
    - PP-Module for Virtual Private Network (VPN) Gateways Version: 1.0 2019-09-17

as clarified by all applicable Technical Decisions.

The TOE is the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 network device.

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

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

The Leidos evaluation team concluded that the product meets the Common Criteria requirements of the collaborative Protection Profile for Network Devices Version 2.1, 24 September- 2018 (NDcPP21), the PP-Module for Stateful Traffic Filter Firewalls Version 1.3 27-September-2019 (MOD_CPP_FW_v1.3), and the PP-Module for Virtual Private Network (VPN) Gateways Version: 1.0 2019-09-17 (MOD_VPNGW_v1.0). The technical information included in this report was obtained from the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-

7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 Security Target Version: 1.0, September 30, 2020 and analysis performed by the validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v9.0
Protection Profiles:	• collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 • PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 • PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019
Security Target	Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 Security Target Version: 1.0, September 30, 2020

Evaluation Technical Report	• Evaluation Technical Report for Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v9.0 Part 1 (Non-Proprietary) Version: 1.0, September 30, 2020 **[ETR-NP-P1]** • Evaluation Technical Report for Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v9.0 Part 2 (Palo Alto Networks Proprietary) ETR Version: 1.0, September 30, 2020 **[ETR-Prop-P2]**
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Palo Alto Networks, Inc.
Developer	Palo Alto Networks, Inc.
Common Criteria Testing Lab (CCTL)	Leidos
CCEVS Validators	Jerome Myers, PhD Marybeth Panock Kenneth Stutterheim

3 TOE Architecture

Note: The following architectural description is based on the description presented in the Security Target.

3.1 Evaluated Platforms

The TOE comprises two main 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 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 control plane includes a dual 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 list of evaluated product details can be found in the Security Target, Table 1, Section 2.2.1, p.14. These models can be grouped into the following sets:

1. PA-220 series
    a. PA-220
    b. PA-220R
2. PA-800 series
    a. PA-820
    b. PA-850
3. PA-3000 series
    a. PA-3020
    b. PA-3050
    c. PA-3060
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
6. PA-7000 series
    a. PA-7050
    b. PA-7080
7. VM-series
    a. VM-50
    b. VM-100
    c. VM-200
    d. VM-300
    e. VM-500
    f. VM-700
    g. VM-1000-HV

3.2 TOE Description

The functionality provided by each of the subsystems is as follows:

Control Plane

The control plane provides all device management functionality, including:

- All management interfaces—supports both direct and remote connection for the web-based GUI/API and CLI using 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 dataplane 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 with policy enforcement.

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.

VM-Series

The VM-Series on specified hardware provides 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 that includes a VMware, Linux KVM or Microsoft Hyper-V hypervisor and an Intel Core or Xeon processor based on the Ivy Bridge, Haswell, or Broadwell microarchitectures that implement Intel Secure Key, and Network Interface Controllers supported by the server.

The following diagram depicts both the hardware and software architecture of the next-generation firewall.

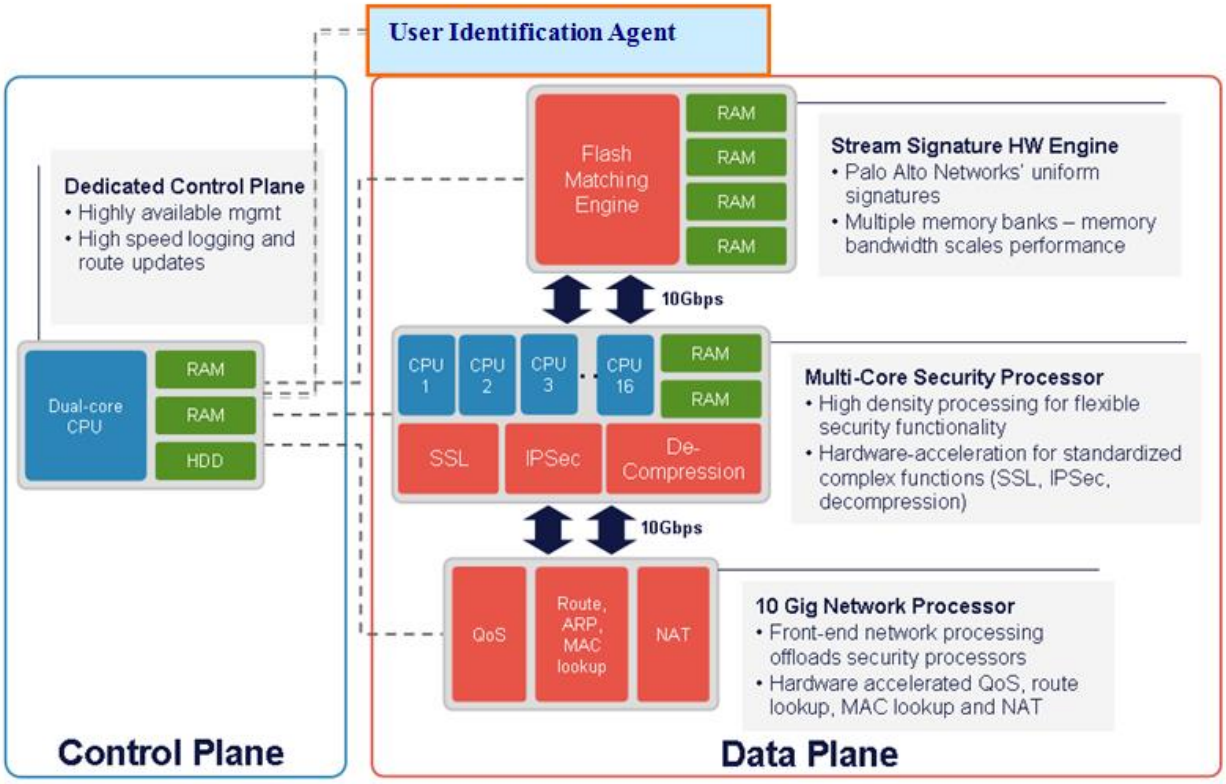


Figure 1: TOE Architecture

3.3 Physical Boundary

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 v9.0.9-h1 – 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-820, PA-850, PA-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, 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-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, 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, and 1 Micro USB Console. 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). Processor: Cavium Octeon CN7130 MIPS64 (DP/MP)
- 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, and 1 Micro USB Console. 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, and 1 Micro USB Console. Processor: Cavium Octeon CN7240 MIPS64 (DP/MP)
- PA-3020/PA-3050: 12 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); 1 RJ-45 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization. Processor: Cavium Octeon CN6335 MIPS64 (DP) / Intel Celeron P4505 (MP)
- PA-3060: 8 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); 1 RJ-45 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization. Processor: Cavium Octeon CN6335 MIPS64 (DP) / Intel Celeron P4505 (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. 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. 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. 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. 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. Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Xeon D1567 (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. Processor: Cavium Octeon CN6880 MIPS64 (DP) / Intel Core i7-2715 (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. Processor: Cavium Octeon CN6880 MIPS64 (DP) / Intel Core i7-2715 (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 Panorama or Wildfire appliances
- Palo Alto Networks Global Protect or UIA application
- Workstation
    - Web browsers - Internet Edge (Release 42 or later), Firefox (version 66.0.5 or later), Safari (version 12.0.3 or later on Mac, and version 5.1.7 or later on Windows and iOS), and Chrome (version 74 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 2008 32-bit and 64-bit, Windows Server 2012, and Windows Server 2012 R2.

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 Final ETR.

4.1 Security Audit

The TOE generates audit records of security relevant events. Generated audit records include the date and time of the event, the event type, the subject identity and the outcome of the event. For audit events resulting from the actions of identified users, the identity of the user is recorded in the generated audit record. The TOE can be configured to store audit records locally so they can be accessed by an administrator and can also be configured to export the audit records to an external audit server.

In the event the space available for storing audit records locally is exhausted, the TOE will overwrite the oldest stored audit records with new audit records as they are generated. The TOE generates an alarm and an audit record to inform the administrator before the local space to store audit data is exhausted and the oldest audit records will start to be overwritten.

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.

4.3 User Data Protection

The TOE ensures 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 (IPsec, HTTPS, SSH) and local connections to the GUI and SSH for interactive administrator sessions and HTTPS for XML and REST API. HTTPS connections can also be tunneled over IPsec.

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

When a user authenticates a local interactive session, no information about the authentication data (i.e., password) is echoed to the user. Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: !; @; #; $; %; ^; &; *; (;); _; <; >; .; ~; '; +; ,; -; /; :; “;”; =; [; \;]; `; {; and }. The TOE supports the use of X.509v3 certificates for IPsec and TLS authentication and also supports certificate revocation checking using Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL).

4.5 Security Management

The TOE provides a Graphical User Interface (GUI) to access its 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 HTTPS, 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.

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 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 audit accountability).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce 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 both local and 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, IPsec, or HTTP over TLS. SSH, IPsec, and TLS ensure both integrity and disclosure protection.

The TOE protects communication with the UIA, Panorama, Global Protect, and Wildfire 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.

4.9 Stateful Traffic Filtering

The TOE implements 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 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.

5 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 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 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 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 functionality).

  In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device 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 ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The authorized 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 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 network 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 network device are protected by the platform on which they reside.
- The Administrator must 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.
- The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device.

The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

- The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- 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 security policies will be enforced on all applicable network traffic flowing among the attached networks.

6 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 assurance activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.1, September 2018, Supporting Document Mandatory Technical Document: PP-Module for Virtual Private Network (VPN) Gateways Version 1.0, 2019-09-17, Supporting Document Mandatory Technical Document: Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, September-2019, Version 1.3,* and performed by the evaluation team).
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 9.2 of this document is excluded from the scope of the evaluation.

7 Documentation

The following documents were available for the evaluation. These documents are developed and maintained by Palo Alto Networks, and are delivered to the end user of the TOE:

- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS 9.0, September 30, 2020
- PAN-OS® Administrator's Guide Version 9.0, March 16, 2020
- VM-Series Deployment Guide Version 9.0, December 2, 2019
- PAN-OS CLI Quick Start Version 9.0, August 21, 2019
- PAN-OS Web Interface Help Version 9.0, Last Revised April 3, 2020
- PAN-OS and Panorama API Usage Guide Version 9.0, Last Revised June 4, 2020.

Palo Alto Networks provides these 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 was examined during the course of the evaluation and delivered with the TOE

The above documents are considered to be part of the evaluated TOE. These documents-, listed above, are the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. Any additional customer documentation delivered with the product or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration. To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above.

Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. The information is derived from the Evaluation Test Report for Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v9.0 Part 2 (Palo Alto Networks Proprietary) ETR Version: 1.0, September 30, 2020 [ETR-Prop-P2] and from the test report for the Palo Alto Pan OS v9.0 network devices, which are listed in the bibliography section 15 of this document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

8.1 Developer Testing

NDcPPv2.1 evaluations do not require developer testing evidence for assurance activities.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP v2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways. The Independent Testing activity is documented in the Assurance Activities Report (AAR), which is publicly available, and is not duplicated here. Test Configuration is covered in the next section below. A test plan was developed in accordance with the Testing Assurance Activities specified in the NDcPPv2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways along with their Supporting Documents. All testing was carried at the Leidos Common Criteria Testing Laboratory, 6841 Benjamin Franklin Drive, Columbia, MD 21046. Testing occurred from September 2, 2019 to June 25, 2020; testing was completed in October 2020. The TOE was located in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was kept with the evaluator at all times.

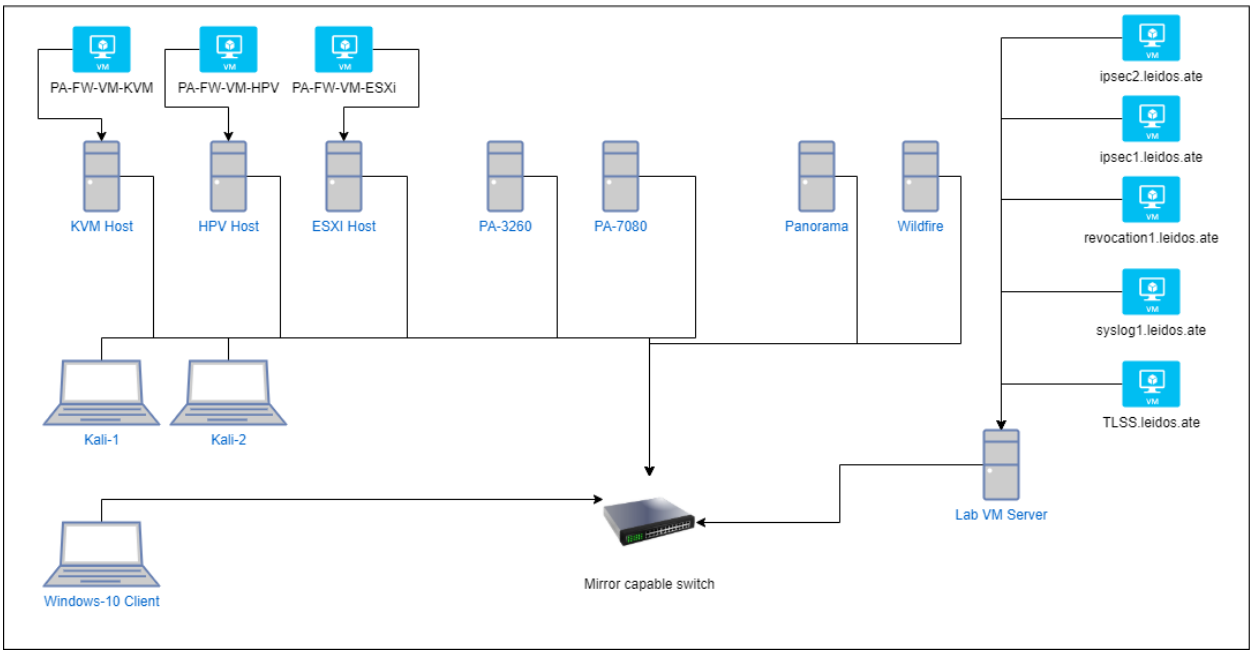
The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by following the preparative procedures
- Successfully executed the NDcPP Assurance-defined tests including the selection-based TLS, and X509 tests
- Planned and executed a series of vulnerability/penetration tests.

It was determined after examining the Test Report and full set of test results provided by the evaluators that the testing requirements for NDcPPv2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways are fulfilled.

8.3 Test Configuration

Evaluation team testing used the TOE configurations depicted in the following figure.



The following components were used to create the test configurations:

- TOE Hardware (Physical)
  - PA-3260
    - MGMT
      - IPv4: 172.16.13.13/16
      - IPv6: 2113:aa1::5
      - MAC: 08:66:1F:01:E4:D2
    - NIC1
      - IPv4: 172.16.14.13/16, 192.168.13.1/24
      - IPv6: 2014::a/16, 2114:aa1::5/32
      - MAC: C4:24:56:ab:d4:4a
    - NIC2
      - IPv4: 173.13.15.1/24
      - IPv6: 2004::1/16
      - MAC: C4:24:56:ab:d4:4b
  - PA-7080
    - MGMT
      - IPv4: 172.16.13.14/16
      - IPv6: 2113:aa1::6/32

- MAC: 08:66:1f:02:c8:d0

- NIC1
  - IPv4: 172.16.14.14/16, 192.168.14.1/24
  - IPv6: 2114:aa1::5/32
  - MAC: d4:1d:71:a6:78:80
- NIC2
  - IPv4: 172.14.15.1/24
  - IPv6: 2005::1/16MAC: d4:1d:71:a6:78:8

- TOE Hardware (Virtual Machines)
  - VMWare ESXi
    - Dell R730 with Intel XEON CPU E5-2640 v4
    - MGMT
      - IPv4: 172.16.13.10/16
      - IPv6: 2113:aa1::2/32
      - MAC: 00:0C:29:02:C9:60
    - NIC1
      - IPv4: 172.16.14.10/24, 192.168.15.1/24
      - IPv6: 2114:aa1::2/32
      - MAC: 00:0c:29:02:c9:6a
    - NIC2
      - IPv4: 172.16.15.10/24, 172.168.0.1/16, 172.10.15.1/24
      - IPv6: 2001::1/16
      - MAC: 00:0c:29:02:c9:74
  - Linux KVM
    - Dell PowerEdge R730 with Intel XEON CPU E5-2640 v4
    - MGMT
      - IPv4: 172.16.13.12/16
      - IPv6: 2113:aa1::4/32
      - MAC: 52:54:00:A7:EB:C4
    - NIC1
      - IPv4: 10.12.14.1/16, 172.16.14.12/24
      - IPv6: 2013::/16, 2114:aa1::4/32
      - MAC: 52:54:00:fd:17:ed
    - NIC2
      - IPv4: 192.168.12.1/24, 172.12.15.1/24

        - IPv6: 2003::/16
        - MAC: 52:54:00:ad:1a:6d
    - Microsoft Hyper-V
        - Dell PowerEdge R730 with Intel XEON CPU E5-2640 v4
        - Dell PowerEdge R730 with Intel Xeon CPU E5-2640 v4
        - MGMT
            - IPv4: 172.16.13.11/16
            - IPv6: 2113:aa1::3/32
            - MAC: 00:15:5D:44:C6:03
        - NIC1
            - IPv4: 10.11.14.1/16, 172.16.14.11/24, 192.168.11.1/24
            - IPv6: 2114:aa1::3/32
            - MAC: 00:15:5d:44:c6:0f
        - NIC2
            - IPv4: 172.11.15.1/24
            - IPv6: 2002::1/16, 2012::1/16
            - MAC: 00:15:5d:44:c6:10
- TOE Software
    - PAN-OS v9.0.9-h1
- Additional Environment Hardware
    - TLSS.leidos.ate
        - IPv4: 172.16.0.25/16
        - MAC: 00:50:56:b1:66:0b
    - Kali Linux #1
        - Used for firewall testing through Ostinator and Python tools.
        - IP/MACs generated by ostinator and varies as needed for Firewall testing.
        - MAC: 5c:26:0a:88:91:f2
    - Kali Linux #2
        - Used for firewall testing through Ostinator and Python tools.
        - IP/MACs generated by ostinator and varies as needed for Firewall testing.
        - MAC: 28:00:03:0E:48:1F
    - Syslog1.leidos.ate
        - IPv4: 172.16.0.30/16
        - IPv6: 2113:aa1::25/32
        - MAC: d2:14:05:39:ea:63
    - Windows 10 Client
        - IPV4: 172.168.1.15/16
        - MAC: F0-92-1C-58-E3-C1
    - ipsec1.leidos.ate
        - IPv4: 172.16.0.35/16, 35.16.0.0/24 (Protected by IPSEC)
        - MAC: fa:40:2a:86:0e:12
    - ipsec2.leidos.ate

        - IPv4: 172.16.0.36/16
        - MAC: 00:50:56:b1:b3:2d
    - revocation1.leidos.ate
        - IPv4: 172.16.1.70/16
        - MAC: 02:23:72:fe:f4:f2

The evaluation team followed the installation and configuration procedures documented in the product guidance to install the TOE in the test environment.

9 TOE Evaluated Configuration

9.1 Evaluated Configuration

The TOE, Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0, consists of the hardware and software components listed below that must be configured in accordance with the Common Criteria Addendum described in Section 7:

- 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 v9.0.9-h1 – 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-820, PA-850, PA-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, 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-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, 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, and 1 Micro USB Console. 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). Processor: Cavium Octeon CN7130 MIPS64 (DP/MP)

- 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, and 1 Micro USB Console. 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, and 1 Micro USB Console. Processor: Cavium Octeon CN7240 MIPS64 (DP/MP)
- PA-3020/PA-3050: 12 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); 1 RJ-45 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization. Processor: Cavium Octeon CN6335 MIPS64 (DP) / Intel Celeron P4505 (MP)
- PA-3060: 8 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); 1 RJ-45 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization. Processor: Cavium Octeon CN6335 MIPS64 (DP) / Intel Celeron P4505 (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. 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. 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. 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. 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. Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Xeon D1567 (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. Processor: Cavium Octeon CN6880 MIPS64 (DP) / Intel Core i7-2715 (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. Processor: Cavium Octeon CN6880 MIPS64 (DP) / Intel Core i7-2715 (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 Panorama or Wildfire appliances
- Palo Alto Networks Global Protect or UIA application
- Workstation
    - Web browsers - Internet Edge (Release 42 or later), Firefox (version 66.0.5 or later), Safari (version 12.0.3 or later on Mac, and version 5.1.7 or later on Windows and iOS), and Chrome (version 74 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 2008 32-bit and 64-bit, Windows Server 2012, and Windows Server 2012 R2.

9.2 Excluded Functionality

The list below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration (unless explicitly stated so). It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in Security Target.

In particular, only the following protocols implemented by the TOE have been tested, and only to the extent specified by the security functional requirements: TLS, HTTPS, SSH, IKE/IPsec. The features below are out of scope.

Table 2 Excluded Features

Feature	Description
Telnet and HTTP Management Protocols	Telnet and HTTP are disabled by default and cannot be enabled in the evaluated configuration. Telnet and HTTP are insecure protocols which allow for plaintext passwords to be transmitted. Use SSH, IPsec, 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	The TLS and SSH decryption policies are not evaluated and therefore, these features are out of scope.
Anti-Virus, Anti-Spyware, Anti-Malware Security Policies	The Anti-Virus, Anti-Spyware, Anti-Malware security policies (i.e., profiles) are not evaluated and therefore, there features are out of scope.
File Blocking, DLP, and URL Filtering Security Policies	The File Blocking, DLP (Data Loss Prevention), and URL Filtering security policies/profiles are not evaluated and therefore, these features are out of scope.
API request over HTTP	By default, the TOE supports API requests over HTTPS or HTTPS tunneled over IPsec. API request over HTTP is disabled and cannot be enabled in the evaluated configuration.
Any features not associated with SFRs in claimed [NDcPP], [FW-Module], and [VPNGW-Module]	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities or products are mentioned in the ST, it is for completeness only.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report (ETR).

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluators performed the Assurance Activities specified in the NDcPP.

10.1 Evaluation of Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP v2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways.

The validators 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.

10.2 Evaluation of Development Documentation (ADV)

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. In addition, the evaluator performed the Assurance Activities specified in the NDcPP v2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways related to the examination of the information contained in the TOE Summary Specification.

The validators 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.

10.3 Evaluation of Guidance Documents (AGD)

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. In addition, the evaluator performed the assurance activities specified in the NDcPP v2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways related to the examination of the information contained in the operational guidance documents.

The validators 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.

10.4 Evaluation of Life Cycle Support Activities (ALC)

The evaluation team found that the TOE was adequately identified.

The validators 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.

10.5 Evaluation of Test Documentation and the Test Activity (ATE)

The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP v2.1, the PP-Module for Stateful Traffic Filter Firewalls, and the PP-Module for Virtual Private Network (VPN) Gateways and recorded the results in a Test Report, as summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators 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.

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

The evaluation team performed a public search for vulnerabilities on 7 April 2020, 6 June 2020, and 30 September 2020 and did not discover any public issues with the TOE. The terms used for the search were as follows:

- Router
- Linux 3.10
- Microarchitectural
- Palo Alto
- PA-220
- PA-220R
- PA-820
- PA-850
- PA-3020
- PA-3050
- PA-3060

- PA-3220
- PA-3250
- PA-3260
- PA-5220
- PA5250
- PA-5260
- PA-5280 -0
- PAN-OS -102

The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The sources of the publicly available information are provided below.

- http://web.nvd.nist.gov/view/vuln/search
- https://securityadvisories.paloaltonetworks.com

Fuzz testing was performed against the product in accordance with Assurance Activities and no residual vulnerabilities were uncovered.

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

10.7 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 test activities 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.

11 Validator Comments/Recommendations

The Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 provides capabilities that are in addition to those evaluated. The validators suggest that the consumer pay attention to the evaluated configuration of the devices as the functionality that was evaluated was scoped exclusively to the security functional requirements specified in the Security Target. Only the functionality implemented by the SFR's within the Security Target was evaluated.

Of note, traffic logging and the use of email notifications and the SNMP and SMTP servers have not been subject to testing in the evaluated configuration.

Also note, as described in the ST, section 3.2 TOE Description, and earlier in this VR, section 2.2 TOE Description, the VM-Series virtual appliance in the evaluated configuration must be installed on a hardware platform as specified in these two referenced TOE Descriptions. The VM version of the TOE may interoperate with a cloud but it cannot be installed in private, public or hybrid cloud computing environments.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The excluded functionality is specified in section 9.2 of this report.

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

12 Annexes

Not applicable

13 Security Target

Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 Security Target, Version 1.0, September 30, 2020.

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Device, Version 2.1, 24 September 1018.

[7] PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019.

[9] PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019.

[11] Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0 Security Target, Version 1.0, September 30, 2020. [ST]

[12] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Firewalls with PAN-OS v9.0, Revision Date: September 30, 2020. [AGD]

[13] PAN-OS® Administrator's Guide Version 9.0, March 16, 2020

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

[15] PAN-OS CLI Quick Start Version 9.0, August 21, 2019

[16] PAN-OS Web Interface Help Version 9.0, Last Revised April 3, 2020

[17] PAN-OS and Panorama API Usage Guide Version 9.0, Last Revised June 4, 2020

[18] Evaluation Technical Report for Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0, Part 2 (Leidos Proprietary), Version 1.0, September 30, 2020. [ETR-Prop-P2]

[19] Evaluation Technical Report for Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v9.0 Part 1 (Non-Proprietary) Version: 1.0, September 30, 2020. [ETR-NP-P1]

[20] Assurance Activities Report for Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.0, Version 1.1, September 30, 2020. [AAR]

[21] Palo Alto Networks PANOS v9.0 Vulnerability Assessment Version: 1.0, September 30, 2020 [AVA]

[22] Palo Alto Pan OS v9.0 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.1, Version 1.0, Dated: September 30, 2020. [DTR]