National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6

Report Number:	**CCEVS-VR-VID10839-2018**
Dated:	**30 April 2018**
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

Jim Donndelinger
Meredith Hennan
Tony Chew
Kenneth Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

List of Figures

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 Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 (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 Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in March 2018.

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

- Evaluation Activities for Network Device cPP, Version 1.0, February 2015 ([6])
- Evaluation Activities for Stateful Traffic Filter Firewalls cPP, Version 1.0, February 2015 ([8]).

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 TOE comprises network firewall appliances and virtual appliances on specified hardware used to manage enterprise network traffic flow using function-specific processing for networking, security, and management. The TOE enables the administrator to specify security policies based on identification of applications seeking access to the protected network. The TOE uses packet inspection and a library of applications to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports.

The focus of the evaluation was on the TOE’s conformance to the security functionality specified in the following documents:

- collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 ([5])
- collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, 27 February 2015 ([7]).

The security functionalities specified in these collaborative Protection Profiles include stateful traffic filtering of network traffic, protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profiles and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([13]) and the associated test report produced by the Leidos evaluation team ([14]).

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 Profiles and that the assurance activities specified in [6] and [8] 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:

- TD0262: NIT Technical Decision for TLS server testing - Empty Certificate Authorities list
- TD0257: NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4
- TD0256: NIT Technical Decision for Handling of TLS connections with and without mutual authentication
- TD0255: NIT Technical Decision for TLS Server Tests - Issue 3: Verification of application of encryption
- TD0235: NIT Technical Decision adding DH group 14 to the selection in FCS_CKM.2
- TD0228: NIT Technical Decision for CA certificates - basicConstraints validation
- TD0227: NIT Technical Decision for TOE acting as a TLS Client and RSA key generation
- TD0226: NIT Technical Decision for TLS Encryption Algorithms
- TD0225: NIT Technical Decision for Make CBC cipher suites optional in IPsec
- TD0224: NIT Technical Decision Making DH Group 14 optional in FCS_IPSEC_EXT.1.11
- TD0223: NIT Technical Decision for "Expected" vs "unexpected" DNs for IPsec Communications
- TD0199: NIT Technical Decision for Elliptic Curves for Signatures
- TD0188: NIT Technical Decision for Optional use of X.509 certificates for digital signatures
- TD0187: NIT Technical Decision for Clarifying FIA_X509_EXT.1 test 1
- TD0186: NIT Technical Decision for Applicability of X.509 certificate testing to IPsec
- TD0185: NIT Technical Decision for Channel for Secure Update
- TD0184: NIT Technical Decision for Mandatory use of X.509 certificates
- TD0182: NIT Technical Decision for Handling of X.509 certificates related to ssh-rsa and remote comms

- TD0181: NIT Technical Decision for Self-testing of integrity of firmware and software
- TD0170: NIT Technical Decision for SNMPv3 Support
- TD0169: NIT Technical Decision for Compliance to RFC5759 and RFC5280 for using CRLs
- TD0168: NIT Technical Decision for Mandatory requirement for CSR generation
- TD0160: NIT Technical Decision for Transport mode and tunnel mode in IPsec communications
- TD0156: NIT Technical Decision for SSL/TLS Version Testing in the NDcPP v1.0 and FW cPP v1.0
- TD0155: NIT Technical Decision for TLSS tests using ECDHE in the NDcPP v1.0.
- TD0154: NIT Technical Decision for Versions of TOE Software in the NDcPP v1.0 and FW cPP v1.0
- TD0153: NIT Technical Decision for Auditing of NTP Time Changes in the NDcPP v1.0 and FW cPP v1.0
- TD0151: NIT Technical Decision for FCS_TLSS_EXT Testing - Issue 1 in NDcPP v1.0
- TD0143: NIT Technical Decision for Failure testing for TLS session establishment in NDcPP and FWcPP
- TD0130: NIT Technical Decision for Requirements for Destruction of Cryptographic Keys
- TD0126: NIT Technical Decision for TLS Mutual Authentication
- TD0125: NIT Technical Decision for Checking validity of peer certificates for HTTPS servers
- TD0117: NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
- TD0116: NIT Technical Decision for a Typo in reference to RSASSA PKCS1v1_5 in NDcPP and FWcPP
- TD0115: NIT Technical Decision for Transport mode and tunnel mode in IPsec communication in NDcPP and FWcPP
- TD0114: NIT Technical Decision for Re-Use of FIPS test results in NDcPP and FWcPP
- TD0113: NIT Technical Decision for testing and trusted updates in the NDcPP v1.0 and FW cPP v1.0
- TD0112: NIT Technical Decision for TLS testing in the NDcPP v1.0 and FW cPP v1.0
- TD0111: NIT Technical Decision for third party libraries and FCS_CKM.1 in NDcPP and FWcPP
- TD0096: NIT Technical Interpretation regarding Virtualization
- TD0095: NIT Technical Interpretations regarding audit, random bit generation, and entropy in NDcPP
- TD0094: NIT Technical Decision for validating a published hash in NDcPP
- TD0090: NIT Technical Decision for FMT_SMF.1.1 Requirement in NDcPP.

1.2 Threats

The ST references the PPs 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 PPs, are as follows:

- 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.

- A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.
- 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.

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-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6
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:	April 2018
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, 27 February 2015
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 TOE.

Evaluation Personnel:

Anthony Apted

Cody Cummins

Bobby Russ

Heather Hazelhoff

Validation Personnel:

Jim Donndelinger
Meredith Hennan
Tony Chew

Kenneth Stutterheim
The Aerospace Corporation

3 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.

3.1 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.

3.2 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 and TLS.

3.3 User Data Protection

The TOE allocates and releases the memory resources used for network packet objects. Both when it receives data from the network and when it transmits data to the network, it ensures that the buffers are not padded out with previously transmitted or otherwise residual information by overwriting unused parts of the buffer with 0s. The TOE thus ensures it does not inadvertently reuse data found in network traffic.

3.4 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 (HTTP over TLS) and direct connections to the GUI for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition and authentication of administrators with username, password, and role (set of privileges), which it uses to authenticate the human user and to associate that user with an authorized role. In addition, the TOE can authenticate users using X509 certificates.

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). The TOE will not accept a certificate if it is unable to establish a connection in order to determine the certificate’s validity.

3.5 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 locally via direct RJ-45 Ethernet cable connection and remotely using an HTTPS client.

3.6 Protection of the TSF

The TOE implements 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.

3.7 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.

3.8 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using IPsec or HTTP over TLS. IPsec and TLS ensure both integrity and disclosure protection.

The TOE protects communication with external IT entities as follows:

- With the User Identification Agent (UIA) and update server using TLS
- With an external audit server using IPsec or TLS.

3.9 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 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).
- The authorized administrators for the 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 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.
- The device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.

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 assurance activities specified in *Evaluation Activities for Network Device cPP* and *Evaluation Activities for Stateful Traffic Filter Firewalls cPP*, 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-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 Security Target*, Version 1.0, 16 March 2018.

- Only the following protocols implemented by the Palo Alto Networks devices have been tested, and only to the extent specified by the security functional requirements: IPsec; IKE; TLS; HTTPS.
- The stateful traffic filtering capabilities of the Palo Alto Networks devices have been tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; FTP. The following protocols identified in ST have not been considered in the evaluation: SMTP; SNMP; SSH. Any additional security-related functional capabilities of the product were not covered by this evaluation, including:
    - Threat prevention capabilities
    - App-ID classification technology
    - Layer 2 switching
    - VLAN capabilities
    - Transparent in-line deployment
    - Telnet.
- The TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- The TOE can be configured to use the following components in its operational environment. However, these components have not been evaluated and their use with the TOE is not covered by this evaluation:
    - Administrator workstation—computer connected either directly or remotely to the appliance's Management port via an RJ-45 Ethernet cable. The Management port is an out-of-band management port that provides access to the GUI via HTTPS. The following browsers are supported: Internet Explorer (IE, Release 7 and later, recommended IE Release 10 and later); Firefox (version 3.6 or later); Safari (version 5 or later); Chrome (version 11 or later)
    - syslog server
    - update server
    - Panorama appliance
    - WildFire appliance
    - GlobalProtect application
    - Domain controller
    - User Identification Agent (UIA).
- 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 following guidance documents:
    - *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS v8.0.6*, Version 1.1, 13 March 2018
    - *Palo Alto Networks PAN-OS Administrator's Guide*, Version 8.0, February 3, 2017
    - *Palo Alto Networks PAN-OS Web Interface Reference Guide*, Version 8.0, February 6, 2017
    - *Palo Alto Networks VM-Series Deployment Guide*, Version 8.0, 30 January 2018.

- The evaluated configuration comprises individual firewalls managed in isolation, and not a distributed solution. Additionally, when deploying the TOE in a virtualized environment, the VM-Series virtual appliance must be the only guest running in the virtualized environment, and no other non-network applications may be running on the VM.

5 Architectural Information

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

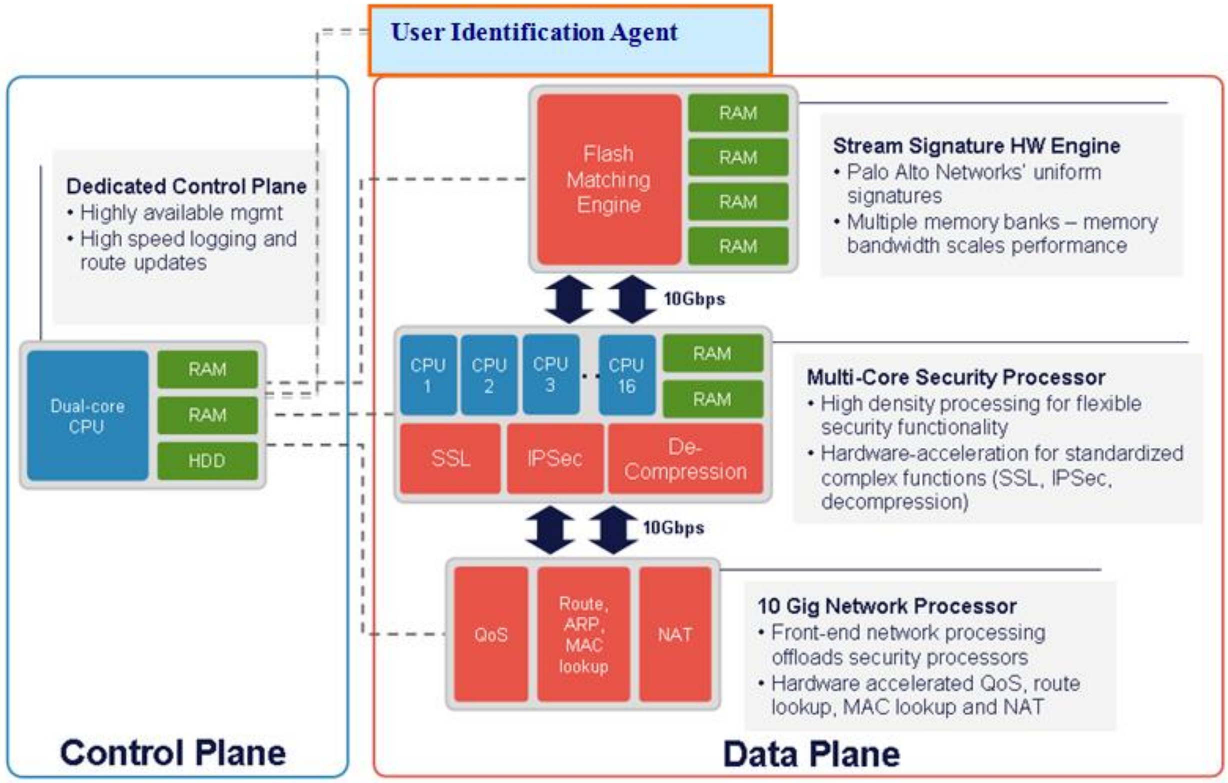
User Identification Agent
Dedicated Control Plane
• Highly available mgmt
• High speed logging and route updates
Dual-core CPU
RAM
RAM
HDD
Control Plane
Flash Matching Engine
RAM
RAM
RAM
RAM
Stream Signature HW Engine
• Palo Alto Networks' uniform signatures
• Multiple memory banks – memory bandwidth 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

Figure 1: TOE Architecture

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
- 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
- Reporting infrastructure for reports, monitoring tools, and graphical visibility tools

- 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
- SSL forward proxy, including decryption and re-encryption
- Policy lookups to determine what security policy to enforce and what actions to take, including scanning for threats, logging, and packet marking
- Application decoding, threat scanning for all types of threats and threat prevention
- 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 functionality as TOE hardware appliances.

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.

6 TOE Evaluated Configuration

6.1 Evaluated Configuration

Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series, Next-Generation Firewall with PAN-OS v8.0.6, as configured in accordance with the guidance documentation listed in Section 7. The specific Firewall appliance models include:

1. PA-200 Series
    a. PA-200
    b. PA-220
2. PA-500
3. PA-800 Series
    a. PA-820
    b. PA-850
4. PA-3000 Series
    a. PA-3020
    b. PA-3050
    c. PA-3060
5. PA-5000 Series
    a. PA-5020
    b. PA-5050
    c. PA-5060
6. PA-5200 Series
    a. PA-5220
    b. PA-5250
    c. PA-5260
7. PA-7000 Series
    a. PA-7050
    b. PA-7080
8. VM-Series - VM-Series
    a. VM-1000-HV
    b. VM-300
    c. VM-200
    d. VM-100
    e. VM-50
    f. VM-500
    g. VM-700

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

- VMware
    - VMware ESXi with vSphere 5.1, 5.5, 6.0, or 6.5
- Linux KVM
    - CentOS/RedHat Enterprise Linux: 7.2.1511 (QEMU-KVM 1.5.3 and libvirt 2.0.0; Open vSwitch: 2.3.1 and later)

- Microsoft Hyper-V Server 2012 R2—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 2012 R2, or as an add-on/role for Windows Server 2012 R2.

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.

The VM-Series virtual appliance must be the only guest running in the virtualized environment.

Evaluation testing included the following:

VMware ESXi 5.5:

- Dell PowerEdge R730 Processor: Intel XEON CPU E5-2640 v4 (Broadwell microarchitecture) with Broadcom 5720 NIC
- Memory: 64 GB ECC DDR4 2133

and

- PacStar PS451 Processor: Intel Xeon CPU E3-1258L v4
- Network Interfaces: Intel I218-LM:MGMT port-vmnic0-, Intel I210: vmnic 1-4 vvv

KVM:

- Dell PowerEdge R730 Server running on an Intel Xeon E5-2630 v3 (Haswell microarchitecture) with Broadcom 5720 NIC
- Memory: 64 GB ECC DDR4 2133

Microsoft Hyper-V:

- Dell PowerEdge R730 Processor: Intel XEON CPU E5-2640 v4 (Broadwell microarchitecture) with Broadcom 5720 NIC
- Memory: 64 GB ECC DDR4 2133

6.2 Excluded Functionality

- Threat prevention capabilities
- App-ID classification technology
- Layer 2 switching
- VLAN capabilities
- Transparent in-line deployment
- Telnet

7 Documentation

Palo Alto Networks 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 course of the evaluation and delivered with the TOE is as follows:

- *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS v8.0.6*, Version 1.1, 13 March 2018
- *Palo Alto Networks PAN-OS Administrator's Guide*, Version 8.0, February 3, 2017
- *Palo Alto Networks PAN-OS Web Interface Reference Guide*, Version 8.0, February 6, 2017
- *Palo Alto Networks VM-Series Deployment Guide*, Version 8.0, 30 January 2018.

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

8 Independent Testing

This section summarizes evaluation team testing of the TOE. It is based on information contained in the proprietary *Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 Test Report and Procedures*, Version 1.0, 16 March 2018 ([14]), as summarized in *Assurance Activities Report for Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6*, Version 1.1, 16 March 2018 ([13]), which is publicly available.

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to:

- *collaborative Protection Profile for Network Devices*, Version 1.0, 27 February 2015
- *collaborative Protection Profile for Stateful Traffic Filter Firewalls*, Version 1.0, 27 February 2015.

The evaluation team devised a test plan based on the Tests evaluation activities specified in:

- *Evaluation Activities for Network Device cPP*, Version 1.0, February 2015
- *Evaluation Activities for Stateful Traffic Filter Firewalls cPP*, Version 1.0, February 2015.

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 of the TOE took place from June 19 to December 1, 2017 at the Leidos CCTL facility in Columbia, Maryland.

8.1 Test Configuration

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

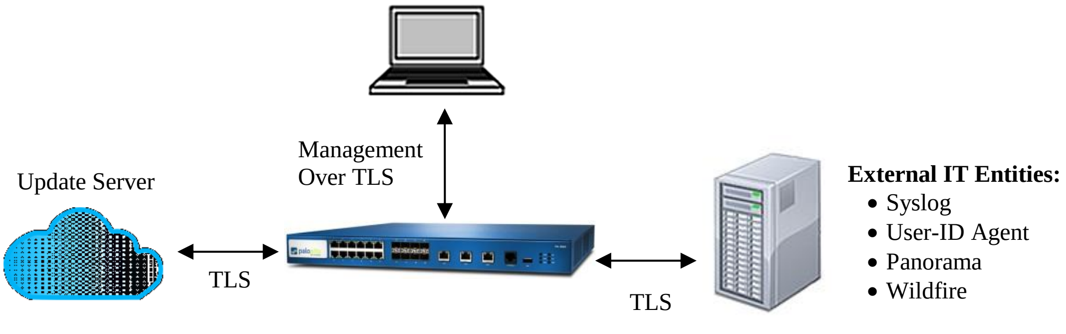

Figure 2: Configuration for General Testing

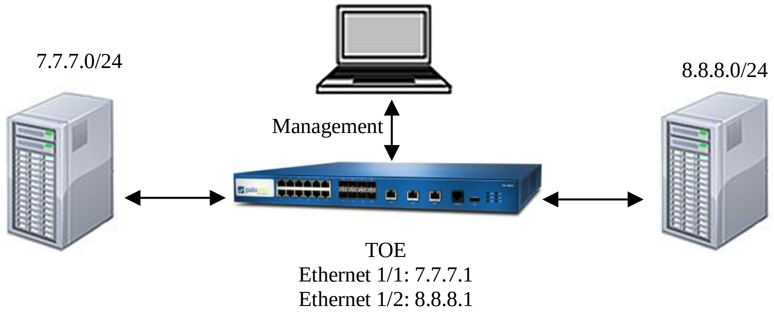

Figure 3: Configuration for Testing Stateful Traffic Filtering

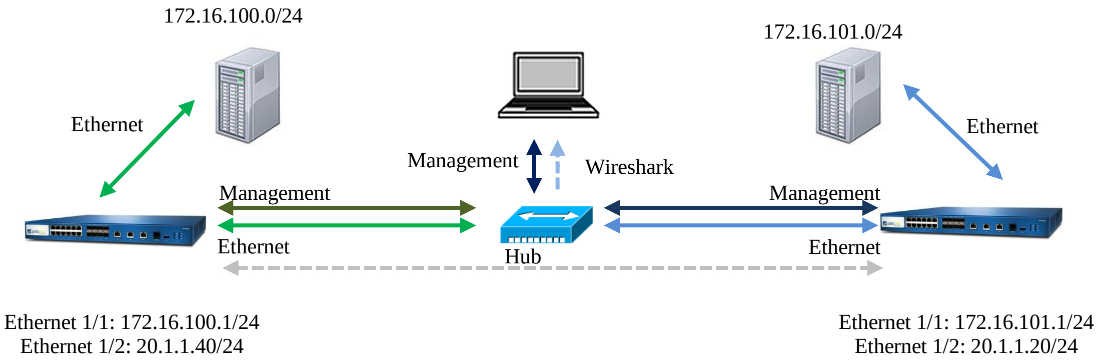
172.16.100.0/24
172.16.101.0/24
Ethernet
Ethernet
Management
Wireshark
Management
Management
Ethernet
Hub
Ethernet
Ethernet 1/1: 172.16.100.1/24
Ethernet 1/2: 20.1.1.40/24
Ethernet 1/1: 172.16.101.1/24
Ethernet 1/2: 20.1.1.20/24

Figure 4: Configuration for Testing IPsec

The following components were used to create the test configurations:

- TOE Hardware (Physical)
  - PA-820 Next Generation Firewall
  - PA-5260 Next Generation Firewall
  - PA 3060 Next Generation Firewall
  - PA-7050 Next Generation Firewall
- TOE Hardware (Virtual Machines)
  - VMWare ESXi 5.5
    - Dell R730 with Intel XEON CPU E5-2640 v4
    - PacStar PS451 with Intel Xeon CPU E3-1258L v4
  - Linux KVM
    - Dell PowerEdge R730 with Intel Xeon E5-2630 v3
  - Microsoft Hyper-V
    - Dell PowerEdge R730 with Intel XEON CPU E5-2640 v4
- TOE Software
  - PAN-OS v8.06
  - VM-300 License
- Additional Environment Hardware
  - Management Workstations with web browsers

    - Syslog Server (rsyslog), also used as TLS testing device
    - PC with User Identification Agent installed
    - Palo Alto Panorama
    - Palo Alto Wildfire
    - Network devices used for packet generation and capture

- Test Hardware
    - Network Test Monitor (one or more computers running evaluation team networking tools).
- Test Software Tools
    - Publicly available tools:
        - Mozilla Firefox version 59.0.2 – used for administrative access to the TOE's web GUI interface
        - Wireshark version 2.2.6 – used for traffic capture to/from the TOE
        - Ostinato version 0.5.1 – used for packet manipulation to test packet filtering and firewall rules
        - OpenSSL s_client and s_server version 1.0.2g – used for the generation and signing of X.509 certificates
    - Proprietary tools:
        - TLS Test Tool (built from the NIAP test tool with some proprietary patches to address test activities that differ between PPs and based on NIAP TD changes issued over the years) – used to perform TLS testing that requires man-in-the-middle packet manipulation

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

Subsequently, the evaluators exercised all the test cases. The tests were selected in order to ensure that each of the test assertions specified in *Evaluation Activities for Network Device cPP* and *Evaluation Activities for Stateful Traffic Filter Firewalls cPP* were covered. All tests passed.

8.2 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]. These searches were performed during the evaluation and then re-performed a final time on April 10, 2018 to ensure that no additional public vulnerabilities were disclosed prior to the completion of the evaluation.

The evaluation team searched the National Vulnerability Database[1] and the vendor's own Security Advisories web page, which can be found at https://securityadvisories.paloaltonetworks.com.

The keyword searches included the following terms:

- "Palo Alto"
- "PAN-OS"

[1] http://web.nvd.nist.gov/view/vuln/search

- “Cavium”
- The terms “router”, “switch” and “firewall”
- The following protocols: “TCP”, “UDP”, “IPv4”, “IPv6”
- The protocols supported through an SFR by the TOE, specifically “IPsec” and “TLS”.

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

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 4 of the CC and CEM:

- *Evaluation Activities for Network Device cPP*, Version 1.0, February 2015
- *Evaluation Activities for Stateful Traffic Filter Firewalls cPP*, Version 1.0, February 2015.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). As stated in the Clarification of Scope, the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. It should be noted that:

- Panorama, Telnet, HTTP, and connections over untrusted networks are not supported and must not be enabled.
- The Captive Portal capability has not been covered in the evaluated configuration and should not be enabled.
- Communication between the TOE and the UIA is protected using TLS and was tested in the evaluation. However, the use of user identities in firewall rule sets is not covered by the scope of evaluation testing.

11 Annexes

Not applicable

12 Security Target

The ST for this product's evaluation is *Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 Security Target*, Version 1.0, 16 March 2018.

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTTP(S)	Hypertext Transfer Protocol (Secure)
IPsec	Internet Protocol Security
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UIA	User Identification Agent
VR	Validation Report

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015.

[6] Evaluation Activities for Network Device cPP, Version 1.0, February 2015.

[7] collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, 27 February 2015.

[8] Evaluation Activities for Stateful Traffic Filter Firewalls cPP, Version 1.0, February 2015.

[9] [empty]

[10] Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 Security Target, Version 1.0, 16 March 2018.

[11] Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS v8.0.6, Palo Alto Networks Next Generation Firewall, Document Version 1.1, 13 March 2018.

[12] Evaluation Technical Report for Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6, Part 2 (Leidos Proprietary), Version 1.1, 16 March 2018.

[13] Assurance Activities Report for Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6, Version 1.1, 16 March 2018.

[14] Palo Alto Networks PA-200 Series, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS v8.0.6 Test Report and Procedures, Version 1.0, 16 March 2018.