National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4

Report Number: CCEVS-VR-VID10640-2015
Dated: November 25, 2015
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

Jean Petty
Jay Vora
The MITRE Corporation

Kelly Hood
Aerospace Corporation

Common Criteria Testing Laboratory

Leidos (formerly SAIC, 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 to determine 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. End-users should also review this Validation Report (VR), which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration, to help in the determination of suitability. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Palo Alto Networks Next-Generation Firewall with PAN-OS 7.0.1-h4, including the PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, and the VM Series installed on hardware specified in the ST. This report describes the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. 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 Next-Generation Firewall Devices with PAN-OS 7.0.1-h4 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in November 2015. 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 and the assurance activities specified in the *Protection Profile for Network Devices, Version 1.1, 8 June 2012*, as amended by Errata #3 – with the optional IPsec, HTTPS, and TLS SFRs, the *Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011*, and the *Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 12 April 2013* as amended by CSfC Selections for VPN Gateways. 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 Leidos evaluation team determined that Palo Alto Networks Next-Generation Firewall Devices with PAN-OS 7.0.1-h4 is conformant to the claimed Protection Profile (PP) and extended packages and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the ST. The information in this VR is largely derived from the publically available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The TOE is Palo Alto Networks next-generation firewall with PAN-OS 7.0.1-h4 in the form of an appliance or virtual appliance. The appliances included in the TOE are:

The specific Firewall appliance models include:

- PA-200
- PA-500
- PA-2000
    - PA-2020
    - PA-2050
- PA-3000
    - PA-3020

  - PA-3050
  - PA-3060
- PA-4000
  - PA-4020
  - PA-4050
  - PA-4060
- PA-5000
  - PA-5020
  - PA-5050
  - PA-5060
- PA-7000
  - PA-7050
  - PA-7080
- VM-Series—the following virtual appliances when installed on a specified hardware platform (see below) that includes VMware ESXi 5.5 hypervisor and an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitectures, which implement Intel Secure Key:

  - VM-1000-HV
  - VM-300
  - VM-200
  - VM-100

  Note, the NDPP specifies requirements for a network device—a device composed of hardware and software that is connected to the network and has an infrastructure role on the network. Therefore, the VM-Series virtual appliances are considered to be in their evaluated configuration only when installed on the following specified hardware platforms and are not evaluated for deployment on any other platforms.

  - Dell PowerEdge R430, R530, R630, R730, R730xd and R930 Servers
  - Equivalent platforms i.e., Intel Ivy Bridge or Haswell-based processor with Broadcom or Intel Network Interface Controllers supported by the server

  In addition, the VM-Series virtual appliance must be the only guest running in the virtualized environment. Evaluation testing included the VM-300 installed on a Dell PowerEdge R730 Server running VMware ESXi 5.5 on an Intel Xeon E5-2630 v3 (Haswell microarchitecture) processor with Broadcom 5720 NIC.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP and EPs had been completed successfully and that the product satisfied all of the security functional and assurance requirements as stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Palo Alto Networks Next-Generation Firewall with PAN-OS 7.0.1-h4, including the PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, and VM Series installed on hardware specified in the ST.
Sponsor & Developer	Palo Alto Networks, Inc. 4401 Great America Parkway Santa Clara, CA 95054
CCTL	Leidos, Inc. Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	November 25, 2015
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	*Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3 dated 3 November 2014 and CSfC Selections for VPN Gateways, Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (STFF) Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (VPNGW) as amended by CSfC Selections for VPN Gateways (CSfC).
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Palo Alto Networks Next-Generation Firewall Devices with PAN-OS 7.0.1-h4 by any agency of the U.S. Government and no warranty of Palo Alto Networks Next-Generation Firewall Devices with PAN-OS 7.0.1-h4 is either expressed or implied.
Evaluation Personnel	Katie Sykes, Evaluation Team Lead Justin Sagurton, Evaluator Cody Cummins, Evaluator Kevin Steiner, Evaluator
Validation Personnel	Jean Petty (The MITRE Corporation), Jay Vora (The MITRE Corporation), Kelly Hood (Aerospace Corporation)

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) 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 information technology 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 identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4 Security Target
ST Version	Version 1.0
Publication Date	November 23, 2015
Vendor and ST Author	Vendor: Palo Alto Networks, Inc. ST Author: Leidos, Inc.
TOE Reference	Palo Alto Networks Next-Generation Firewall with PAN-OS 7.0.1-h4, including the PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, and VM Series installed on hardware specified in the ST.
TOE Hardware Models	The appliance models are: 1. PA-200 2. PA-500 3. PA-2000: PA-2020, PA-2050 4. PA-3000: PA-3020, PA-3050, PA-3060 5. PA-4000: PA-4020, PA-4050, PA-4060 6. PA-5000: PA-5020, PA-5050, PA-5060 7. PA-7000: PA-7050, PA-7080 8. VM-Series: VM-300, VM-200, VM-100, VM-1000-HV when installed on the hardware platforms specified in the ST that include VMware ESXi 5.5 hypervisor and an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitectures, which implement Intel Secure Key
TOE Software Version	PAN-OS 7.0.1-h4
Keywords	Firewall, Virtual Private Network, VPN Gateway

2.1 Threats

The Security Target includes by reference the Security Problem Definition from the NDPP with STFF and VPNGW. The TOE and its operational environment are intended to counter the threats described in the following subsections.

2.1.1 Threats from Protection Profile for Network Devices

2.1.1.1 Communications with the TOE

Network devices communicate with other network devices, as well as administrators, over the network. The endpoints of the communication can be both geographically and logically distant from the TOE, and pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications with the TOE to be compromised. While these communications fall into three distinct categories (the TOE communicating with a remote administrator; the TOE communicating in a distributed processing environment with another instance or instances of itself; and the TOE communicating with another IT entity that is not another instance of the TOE (e.g., an NTP server or a peer router)), the threats to the communication between these endpoints are the same.

Plaintext communication with the TOE may allow critical data (such as passwords, configuration settings, and routing updates) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE. Several protocols can be used to provide protection; however, each of these protocols have myriad options that can be implemented and still have the overall protocol implementation remain compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises.

Even though the communication path is protected, there is a possibility that the external entity (be it a remote administrator, another instance of the distributed TOE, or a trusted IT entity such as a peer router) could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the external entity as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate remote entity when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and "playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.

2.1.1.2 Malicious "Updates"

Since the most common attack vector used involves attacking unpatched versions of software containing well-known flaws, updating network device firmware is necessary to ensure that changes to threat environment are addressed. Timely application of patches ensures that the system is a "hard target", thus increasing the likelihood that product will be able to maintain and enforce its security policy. However, the updates to be applied to the product must be trustable in some manner; otherwise, an attacker can write their own "update" that instead contains malicious code of their choosing, such as a rootkit, bot, or

other malware. Once this "update" is installed, the attacker then has control of the system and all of its data.

Methods of countering this threat typically involve hashes of the updates, and potentially cryptographic operations (e.g., digital signatures) on those hashes as well. However, the validity of these methods introduces additional threats. For instance, a weak hash function could result in the attacker being able to modify the legitimate update in such a way that the hash remained unchanged. For cryptographic signature schemes, there are dependencies on

1) the strength of the cryptographic algorithm used to provide the signature, and
2) the ability of the end user to verify the signature (which typically involves checking a hierarchy of digital signatures back to a root of trust (a certificate authority)).

If a cryptographic signature scheme is weak, then it may be compromised by an attacker and the end user will install a malicious update, thinking that it is legitimate. Similarly, if the root of trust can be compromised, then a strong digital signature algorithm will not stop the malicious update from being installed (the attacker will just create their own signature on the update using the compromised root of trust, and the malicious update will then be installed without detection).

2.1.1.3 Undetected System Activity

While several threats are directed at specific capabilities of the TOE, there is also the threat that activity that could indicate an impending or on-going security compromise could go undetected.

Administrators can unintentionally perform actions on the TOE that compromise the security being provided by the TOE; for instance, a mis-configuration of security parameters. Processing performed in response to user data (for example, the establishment of a secure communications session, cryptographic processing associated with a protected session) may give indications of a failure or compromise of a TOE security mechanism (e.g., establishment of a session with an IT entity when no such sessions should be taking place). When indications of activity that may impact the security of the TOE are not generated and monitored, it is possible for harmful activity to take place on the TOE without responsible officials being aware and able to correct the problem. Further, if no data are kept or records generated, reconstruction of the TOE and the ability to understand the extent of any compromise could be negatively affected.

While this PP requires that the TOE generates the audit data, these data are not required to be stored on the TOE, but rather sent to a trusted external IT entity (e.g., a syslog server). These data may be read or altered by an intervening system, thus potentially masking indicators of suspicious activity. It may also be the case that the TOE could lose connectivity to the external IT entity, meaning that the audit information could not be sent to the repository.

2.1.1.4 Accessing the TOE

In addition to the threats discussed in Section 2.1 dealing with the TOE communicating with various external parties that focus on the communications themselves, there are also threats that arise from attempts to access the TOE, or the means by which these access attempts are accomplished.

For example, if the TOE does not discriminate between administrative users that are allowed to access the TOE interactively (through a locally connected console, or with a session-oriented protocol such as SSH) and an administrative user with no authority to use the TOE in this manner, the configuration of the TOE cannot be trusted. Assuming that there is this distinction, there is still the threat that one of the allowed accounts may be compromised and used by an attacker that does not otherwise have access to the TOE.

One vector for such an attack is the use of poor passwords by authorized administrators of the TOE. Passwords that are too short, are easily-guessed dictionary words, or are not changed very often, are susceptible to a brute force attack. Additionally, if the password is plainly visible for a period of time

(such as when a legitimate user is typing it in during logon) then it might be obtained by an observer and used to illegitimately access the system.

Once a legitimate administrative user is logged on, there still are a number of threats that need to be considered. During the password change process, if the TOE does not verify that it is the administrative user associated with the account changing the password, then anyone can change the password on a legitimate account and take that account over. If an administrative user walks away from a logged-in session, then another person with no access to the device could sit down and illegitimately start accessing the TOE.

2.1.1.5 User Data Disclosure

While most of the threats contained in this PP deal with TSF and administrative data, there is also a threat against user data that all network devices should mitigate. Data traversing the TOE could inadvertently be sent to a different user; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the TOE in the course of processing network traffic that could be inadvertently re-used in sending network traffic to a user other than that intended by the sender of the original network traffic.

2.1.1.6 TSF Failure

Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

2.1.2 Threats from Stateful Traffic Filter Firewall Extended Package

Stateful Traffic Filter Firewalls address a range of security threats related to infiltration into a protected network and exfiltration from a protected network. The term protected network is used here to represent an attached network for which rules are defined to control access. As such, a given Stateful Traffic Filter Firewall could potentially have a variety of attached protected and unprotected networks simultaneously depending on its specific configuration. Also, it should be clear that all attached networks are presumed to be protectable at the discretion of an authorized administrator.

The term ingress traffic is used below to represent traffic from threat agents that exist outside a protected network and the term egress traffic is used below to represent traffic from threat agents that exist inside a protected network. Applicable threats include unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. However, relative to the data, it does not matter where the threat agent is located. Example: data exfiltration means that data was removed without proper authorization to remove it. That can be a pull or a push. It can result from intrusion from the outside or by the actions of the insider. A site is responsible for developing its security policy and configuring a ruleset that the firewall will enforce to meet their needs.

2.1.2.1 Unauthorized Disclosure of Information

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.

From an infiltration perspective, Stateful Traffic Filter Firewalls serve to limit access to only specific destination network addresses and ports within a protected network. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information.

From an exfiltration perspective, Stateful Traffic Filter Firewalls serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are routed through authorized proxies or filters to further mitigate inappropriate disclosure of data through extrusion.

2.1.2.2 Inappropriate Access to Services

Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.

From an ingress perspective, Stateful Traffic Filter Firewalls can be configured so that only those network servers intended for external consumption are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network.

From an egress perspective, Stateful Traffic Filter Firewalls can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers. Note that the effectiveness of a Stateful Traffic Filter Firewall is rather limited in this regard since external servers can offer their services on alternate ports – this is where an Application Filter Firewall offers more reliable protection, for example.

2.1.2.3 Misuse of Services

Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.

From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, Stateful Traffic Filter Firewalls can log policy violations that might indicate violation of publicized usage statements for publicly available services.

From an egress perspective, Stateful Traffic Filter Firewalls can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a Stateful Traffic Filter Firewall can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, Stateful Traffic Filter Firewalls can be configured to log network usages that

cross between protected and external networks and as a result can serve to identify potential usage policy violations.

2.1.2.4 Disruption or Denial of Services

Stateful Traffic Filter Firewalls may be vulnerable to denial of services (DOS) attacks related to resource exhaustion in the event of coordinated service request flooding originating from outside of the protected network.

From an ingress perspective, Stateful Traffic Filter Firewalls can be configured so that only those network servers intended for external consumption are accessible and only via the intended ports and as a result potential attacks can be limited to select servers and services that have been configured (e.g., 'hardened') for that purpose. This serves to reduce available attack surface and mitigate the potential for external network attacks against internal servers. Attacks against even those servers that are externally accessible would be limited to the configured ports reducing the possible attack vectors.

From an egress perspective, Stateful Traffic Filter Firewalls can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network. For example, access to external mail servers can be blocked to reduce the chance of e-mail based attacks that might serve to introduce viruses, malware, etc. ultimately resulting in disruption of services on a protected network. Note that the effectiveness of a Stateful Traffic Filter Firewall is rather limited in this regard since external servers can offer their services on alternate ports – this is where an Application Filter Firewall offers more reliable protection, for example. However, logging can serve to help identify service disruptions that have not been prevented (e.g., by detecting the spread of viruses or 'botnet' activity patterns).

2.1.3 Threats from VPN Gateway Extended Package.

VPN Gateways address a range of security threats related to the confidentiality and integrity of data that traverses an untrusted network such as infiltration into a protected network and exfiltration from a protected network. The term protected network is used here to represent an attached network for which rules are defined to control access. As such, a given VPN could potentially have a variety of attached protected and unprotected networks simultaneously depending on its specific configuration. It should also be clear that all attached networks are presumed to be protectable at the discretion of an administrator. The term ingress traffic is used below to represent traffic from threat agents that exist outside a protected network and the term egress traffic is used below to represent traffic from threat agents that exist inside a protected network. Applicable threats include unauthorized disclosure of information, inappropriate access to services, and network-based reconnaissance. However, relative to the data, it does not matter where the threat agent is located. Example: data exfiltration means that data was removed without proper authorization to remove it. This may be a pull or a push. It can result from intrusion from the outside or by the actions of the insider. A site is responsible for developing its security policy and configuring a rule set that the VPN will enforce to meet their needs.

2.1.3.1 Unauthorized Disclosure of Information

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.

From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or

transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information.

From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.

2.1.3.2 Inappropriate Access to Services

Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.

From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network.

From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link.

2.1.3.3 Misuse of Services

Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.

From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services.

From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a Stateful Traffic Filter Firewall can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.

2.1.3.4 Compromise of Data Integrity

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the

protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.

2.1.3.5 Replay Attack

If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver.

2.2 Organizational Security Policies

The Security Target includes by reference the Security Problem Definition from the NDPP with STFF and VPNGW. The organizational security policies defined in the subsections below apply to the TOE.

2.2.1 Policies from Protection Profile for Network Devices

2.2.1.1 P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

2.2.2 Policies from Stateful Traffic Filter Firewall Extended Package

No organizational policies have been identified that are specific to Stateful Traffic Filter Firewalls.

2.2.3 Policies from VPN Gateway Extended Package.

No organizational policies have been identified that are specific to VPN Gateways.

3 Architectural Information

The architecture of Palo Alto Network next-generation firewall is divided into three subsystems: the control plane; the data plane; and the User Identification Agent (UIA). The control plane provides system management functionality while the data plane handles all data processing on the network. Both the control plane and the data plane reside on the firewall appliance. The User Identification Agent is installed on a separate dedicated PC on the network and communicates with a domain controller to retrieve user-specific information. The User Identification Agent allows the next-generation firewall to automatically collect user information and include it in policies and reporting.

Figure 1 below depicts both the hardware and software architecture of the next-generation firewall. The User Identification Agent is in the operational environment.

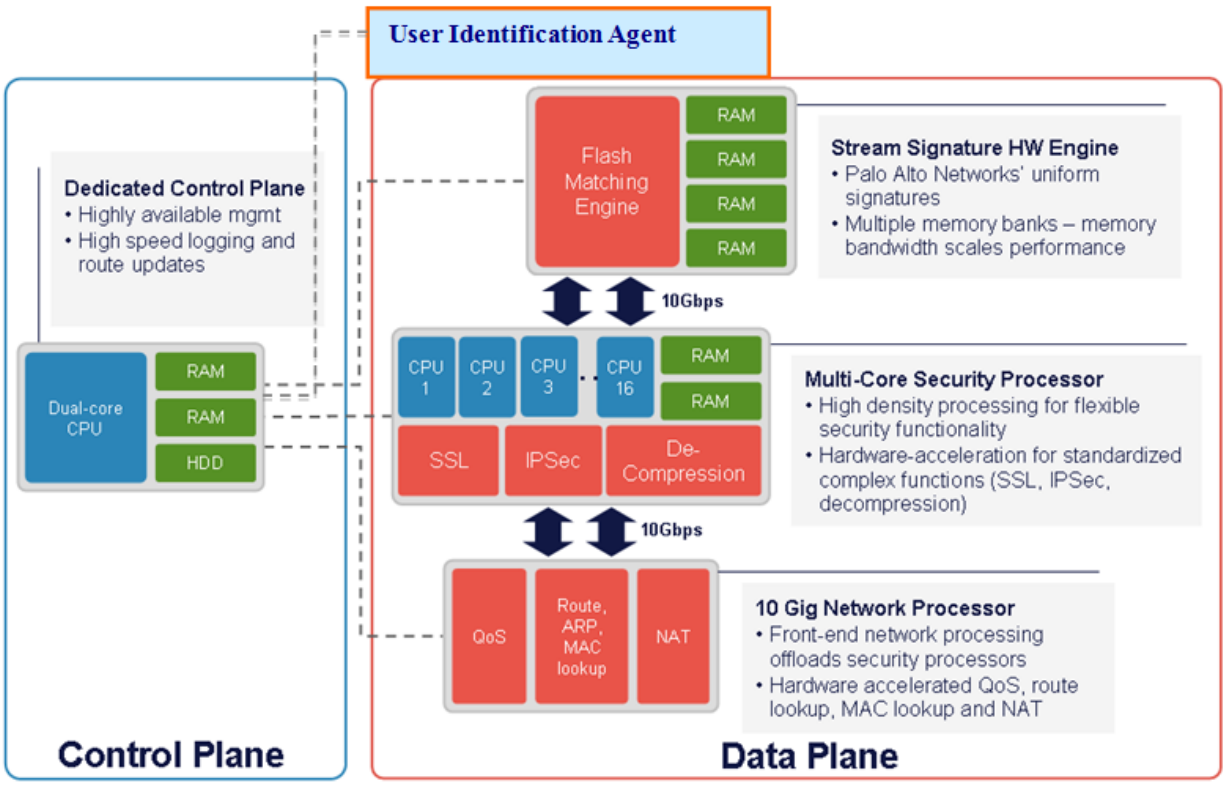

Figure 1 TOE Architecture

3.1 Firewall Subsystems

The functionality provided by each subsystem of the TOE is summarized as follows.

3.1.1 Control Plane

The control plane provides all device management functionality, including:

- All management interfaces – provide a both direct and remote connection for the Web Interface GUI.

- 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 for policy enforcement.

3.1.2 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

The product's SSL decryption feature uses an SSL proxy to establish itself as a man-in-the-middle proxy, which decrypts and controls the traffic within the SSL tunnel that traverses the TOE. The SSL proxy acts as a forward proxy (internal client to an external server).

SSH Decryption is checked using the SSH application signature. A policy lookup will occur on the decrypt rule to see if this session should be decrypted. If yes, the TOE will set up a man-in-the middle to decrypt the session and decide if any port-forwarding request is sent in that session. As soon as any port forwarding is detected, the application becomes an SSH-tunnel, and based on the policy, the session might get denied.

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

3.1.3 User Identification Agent

The user identification agent is a client software program installed on one or more PCs on the protected network to obtain user-specific information. The agent can be installed on any PC running Windows Vista, or Windows Server 2003 32-bit with SP2 (or higher than SP2), or Windows Server 2008 32-bit and 64-bit. The agent communicates with a Microsoft Windows Domain Controller to obtain user information (such as user groups, users, and machines deployed in the domain) and makes the information available to the firewall. The firewall uses the information for policy enforcement and reporting. The UIA maintains mapping information received from the Domain Controller, which it synchronizes to the firewall table. The UIA provides the firewall with the capability to automatically collect user-specific information, and provides mapping information between IP addresses and network users. Policy enforcement decisions regarding whether or not a packet is allowed through the firewall are made based on the packet's IP addresses. The UIA allows firewall policies to be constructed using user identifiers as well as IP addresses. The use of user identities in firewall rule sets is not covered by the scope of evaluation testing. The UIA only works with IPv4 addresses and does not work with IPv6 addresses. The User Identification Agent is in the operational environment.

3.2 VM-Series

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

Automation features such as VM monitoring, dynamic address groups and a REST-based API permit proactively monitoring VM changes and dynamically feeding that context into security policies, thereby eliminating the policy lag that may occur when your VMs change.

Each VM-Series virtual appliance in its evaluated configuration is installed on a hardware platform as specified below, including the VMware ESXi 5.5 hypervisor, an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitectures that implement Intel Secure Key, and Network Interface Controllers supported by the Server. Hardware platforms are:

- Dell PowerEdge R430, R530, R630, R730, R730xd and R930 Servers
- Equivalent platforms i.e., Intel Ivy Bridge or Haswell-based processor with Broadcom or Intel Network Interface Controllers supported by the server

In addition, the VM-Series virtual appliance must be the only guest running in the virtualized environment. Evaluation testing included the VM-300 installed on a Dell PowerEdge R730 Server running VMware ESXi 5.5 on an Intel Xeon E5-2630 v3 (Haswell microarchitecture) processor with Broadcom 5720 NIC.

.

4 Assumptions and Clarification of Scope

The ST includes by reference the Security Problem Definition from the NDPP with STFF and VPNGW. The following secure usage assumptions apply in the operational environment of the TOE.

4.1 Assumptions

4.1.1 Assumptions from Protection Profile for Network Devices

4.1.1.1 A.NO_GENERAL_PURPOSE

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

4.1.1.2 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

4.1.1.3 A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.1.2 Assumptions from Stateful Traffic Filter Firewall Extended Package

4.1.2.1 A.CONNECTIONS

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.

4.1.3 Assumptions from VPN Gateway Extended Package.

4.1.3.1 A.CONNECTIONS

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.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. 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.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. 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.

5. The NDPP specifies that the TOE must consist of a device composed of hardware and software that is connected to the network and has an infrastructure role on the network. Therefore, the VM-Series virtual appliances alone were not evaluated. The VM-Series virtual appliances are considered to be in their evaluated configuration only when installed on the specified hardware platforms specified below that include VMware ESXi 5.5 hypervisor and an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitectures, which implement Intel Secure Key.

    - Dell PowerEdge R430, R530, R630, R730, R730xd and R930 Servers
    - Equivalent platforms i.e., Intel Ivy Bridge or Haswell-based processor with Broadcom or Intel Network Interface Controllers supported by the server

    In addition, the VM-Series virtual appliance must be the only guest running in the virtualized environment. Evaluation testing included the VM-300 installed on a Dell PowerEdge R730 Server running VMware ESXi 5.5 on an Intel Xeon E5-2630 v3 (Haswell microarchitecture) processor with Broadcom 5720 NIC. The reader is strongly cautioned that the VM-series virtual appliances were not evaluated for deployment on any other platforms.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Security Audit

The TOE is designed to be able to generate logs for a wide range of security relevant events including the events specified in NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator and can also be configured to send the logs to a designated external log server.

5.2 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. Note that to be in the evaluated configuration, the TOE must be configured in Common Criteria mode, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

5.3 User Data Protection

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

5.4 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 and can be configured to lock a user out after a configurable number of unsuccessful authentication attempts.

5.5 Security Management

The TOE provides a GUI to access the wide range of 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/TLS 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 create new user accounts, configure the audit function, configure the information flow control rules, and review the audit trail. The TOE provides pre-defined Security Administrator, Audit Administrator, and Cryptographic Administrator roles. These administrator roles are all considered Security Administrator as defined in the NDPP for the purposes of this ST.

5.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE includes functions to perform self-tests so that it 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.

5.7 TOE access

The TOE provides the capabilities for both TOE- and user-initiated locking of interactive sessions and for TOE termination of an interactive session after a period of inactivity. The TOE will display an advisory and consent warning message regarding unauthorized use of the TOE before establishing a user session.

5.8 Trusted Path/Channels

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

The TOE protects communication with the UIA, update server 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.

5.9 Stateful traffic filtering

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

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

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

5.10 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.

6 Documentation

Palo Alto Networks offers guidance documents describing the installation process for the TOE as well as guidance for subsequent use and administration 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 PAN-OS Administrator's Guide Version 7.0
- Palo Alto Networks Web Interface Reference Guide Version 7.0
- Common Criteria Evaluated Configuration Guide, Palo Alto Networks Next Generation Firewall, Document Version 1.0, November 23, 2015

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4 Security Target

7 Independent Testing

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

- *Evaluation Team Test Report for Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4*

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the NDPP with STFF and VPNGW extended packages.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the NDPP and the STFF and VPNGW extended packages. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

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

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the NDPP with STFF and VPNGW extended packages were fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE consists of Palo Alto Networks next-generation firewall with PAN-OS 7.0.1-h4 running on any of the following physical appliances:

9. PA-200
10. PA-500
11. PA-2020
12. PA-2050
13. PA-3020
14. PA-3050
15. PA-3060
16. PA-4020
17. PA-4050
18. PA-4060
19. PA-5020
20. PA-5050
21. PA-5060
22. PA-7050
23. PA-7080

The evaluated version of the TOE also includes VM-Series models VM-100, VM-200, VM-300, and VM-1000-HV only when installed on the hardware platforms specified below that include VMware ESXi 5.5 hypervisor and an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitectures, which implement Intel Secure Key. The hardware platforms are:

- Dell PowerEdge R430, R530, R630, R730, R730xd and R930 Servers
- Equivalent platforms i.e., Intel Ivy Bridge or Haswell-based processor with Broadcom or Intel Network Interface Controllers supported by the server

In addition, the VM-Series virtual appliance must be the only guest running in the virtualized environment. Evaluation testing included the VM-300 installed on a Dell PowerEdge R730 Server running VMware ESXi 5.5 on an Intel Xeon E5-2630 v3 (Haswell microarchitecture) processor with Broadcom 5720 NIC.

The TOE must be deployed as described in section 4 Assumptions of this document and be configured in accordance with the *Palo Alto Networks PAN-OS Administrator's Guide Version 7.0* and *Palo Alto Networks Web Interface Reference Guide Version 7.0*.

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the NDPP with STFF and VPNGW extended packages in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

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 PP [6] and EPs [7] [8], 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 3: 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 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 Palo Alto Networks Next-Generation Firewall Devices with PAN-OS 7.0.1-h4, 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.

The product contains more functionality than was covered by the evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Potential users of the VM-Series product included in this evaluation are strongly cautioned that this product includes both hardware and software. For the VM-Series models of the TOE, including VM-Series models VM-100, VM-200, VM-300, and VM-1000-HV, the evaluated configuration consists of the VM-Series model installed on the hardware platforms specified below that include VMware ESXi 5.5 hypervisor and an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitectures, which implement Intel Secure Key. The hardware platforms are:

- Dell PowerEdge R430, R530, R630, R730, R730xd and R930 Servers
- Equivalent platforms i.e., Intel Ivy Bridge or Haswell-based processor with Broadcom or Intel Network Interface Controllers supported by the server

In addition, the VM-Series virtual appliance must be the only guest running in the virtualized environment. Any other configuration or installation of the VM-Series virtual appliances has not been evaluated and is not included in the evaluated configuration.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4 Security Target
ST Version	Version 1.0
Publication Date	November 23, 2015

13 Abbreviations and Acronyms

AAA	Authentication, Authorization and Accounting
AAR	Assurance Activities Report
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	CC Testing Laboratory
CEM	Common Methodology for IT Security Evaluation
CLI	Command Line Interface
CSfC	Commercial Solutions for Classified
DEP	Data Execution Prevention
EP	Extended Package
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IOS	Inter-network Operating System
IPsec	Internet Protocol security
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SA	Security Association
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF	TOE Security Functions
TSS	TOE Summary Specification
UIA	User Identification Agent
USB	Universal Serial Bus
VPN	Virtual Private Network
VR	Validation Report
WAN	Wide Area Network

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] *Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.*

[6] *Protection Profile for Network Devices, Version 1.1, 8 June 2012*

[7] *Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011*

[8] *Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 as amended by CSfC Selections for VPN Gateways (CSfC).*

[9] *Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4 Security Target, Version 1.0, November 23, 2015*

[10] *Palo Alto Networks PAN-OS Administrator's Guide Version 7.0, 9 June, 2015*

[11] *Palo Alto Networks Web Interface Reference Guide Version 7.0, 29 May, 2015*

[12] *Common Criteria Evaluated Configuration Guide, Palo Alto Networks Next Generation Firewall, Document Version 1.0, November 23, 2015*

[13] *Evaluation Team Test Report for Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4, Version 0.5, November 23, 2015*

[14] *Assurance Activities Report for Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS 7.0.1-h4, Version 0.4, November 23, 2015*