National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2

Report Number: CCEVS-VR-VID10392-2013
Dated: 21 April 2013
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

Daniel Faigin

The Aerospace Corporation
El Segundo, CA

Jerome F. Myers

The Aerospace Corporation
Columbia, MD

Alan Arehart

The Aerospace Corporation
El Segundo, CA

Common Criteria Testing Laboratory

SAIC
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in April 2013. 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 2. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Conformant and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4 augmented with ALC_FLR.2 and ATE_DPT.3. The information in this Validation Report derives largely from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The Target of Evaluation (TOE) is Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall devices comprising model appliances PA-500, PA-2020, PA-2050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060 running PAN-OS v4.0.12-h2. The TOE also includes the User Identification Agent client v3.1.2.

The TOE is a firewall that provides policy-based application visibility and control to protect traffic flowing through the enterprise network. The TOE is used to manage enterprise network traffic flows using function specific processing for networking, security, and management. The next-generation firewalls identify the applications that are flowing across the network irrespective of port, protocol, or SSL encryption. Administrators can specify security policies based on an accurate identification of each application seeking access to the protected network. The firewalls use 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 purpose of the User Identification Agent component is to provide the firewall with the capability to collect user-specific information that it uses in security policies and reporting automatically.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2 Security Target (ST).

1.1 Evaluation Details

Table 1. Evaluation Details

Evaluated Product:	The Target of Evaluation (TOE) is Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall devices comprising: • The model appliances PA-500, PA-2020, PA-2050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060 running PAN-OS v4.0.12-h2 • The TOE also includes the User Identification Agent client version 3.1.2.
Sponsor:	**Palo Alto Networks Inc.** 3300 Olcott St Santa Clara, CA 95054
Developer:	**Palo Alto Networks Inc.** 3300 Olcott St Santa Clara, CA 95054
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	16 November 2009
Completion Date:	15 April 2013
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 2, September 2007.
Evaluation Class:	EAL 4 augmented with ALC_FLR.2 and ATE_DPT.3
Description:	The PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall devices provide policy-based application visibility and control to protect traffic flowing through the enterprise network. The firewalls identify the applications that are flowing across the network irrespective of port, protocol, or SSL encryption. Administrators can specify security policies based on an accurate identification of each application seeking access to the protected network. The firewall 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 purpose of the User Identification Agent component is to provide the firewall with the capability to collect user-specific information that it uses in policies and reporting automatically.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall devices product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

PP:	Although there is no formal compliance claim, the ST and the TOE it describes do demonstrably meet all of the Security Functional Requirements (SFRs) of the following Protection Profile (PP): • U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1, July 25, 2007.
Evaluation Personnel:	*Science Applications International Corporation*: Katie Sykes Chris Keenan James Arnold Quang Trinh
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operating environment are intended to counter:

- A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
- An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
- An administrator's intentions may become malicious resulting in user or TSF data being compromised.
- A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
- A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.
- A user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.
- Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.
- Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
- Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered.

- A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).
- A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
- A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.
- An entity may misrepresent itself as the TOE to obtain authentication data.
- A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
- A user may gain unauthorized access to an unattended session.
- A user may gain access to services (by sending data through or to the TOE) for which they are not authorized according to the TOE security policy.
- The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
- When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

2 Identification

The evaluated product is **Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall** devices comprising:

- The model appliances PA-500, PA-2020, PA-2050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060 running PAN-OS v4.0.12-h2
- User Identification Agent client, version 3.1.2

3 Security Policy

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

Note: *Much of the description of the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall devices security policy has been extracted and reworked from the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2 Security Target and Final ETR.*

3.1 Security Audit

The TOE provides the capability to generate audit records of a number of security events including all user identification and authentication, configuration events, and information flow

control events (i.e. decisions to allow and/or deny traffic flow). The management GUI is used to review the audit trail. The management GUI offers options to sort and search the audit records, and to include or exclude auditable events from the set of audited events. The TOE stores the audit trail locally. The TOE protects the audit trail by providing only restricted access to it; by not providing interfaces to modify the audit records. The TOE also provides a time-stamp for the audit records. In addition, the TOE monitors various events occurring on the firewall (such as authentication failures and information flow policy failures) and will generate an alarm if the number of such events reaches a configured limit, indicating a potential security violation.

3.2 Identification and Authentication

The TOE ensures that all users accessing the TOE user interfaces are identified and authenticated. The TOE accomplishes this by supporting local user authentication using an internal database. The TOE maintains information that includes 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 be configured to lock a user out after a configurable number of unsuccessful authentication attempts.

3.3 Cryptographic Support

The TOE provides FIPS approved key management capabilities and cryptographic algorithms that are implemented in a FIPS 140-2 validated crypto-module (Certificate #1877). These support the provision of: trusted paths to remote administrators accessing the TOE via HTTPS; trusted channels to authorized external IT entities; SSL decryption; SSH decryption; and protection of TSF data communicated between the firewall device and the User Identification Agent.

3.4 User Data Protection

The TOE enforces the Unauthenticated Information Flow SFP to control the type of information that is allowed to flow through the TOE and the Unauthenticated TOE Services SFP to control access to services offered by the TOE. The enforcement process for these SFPs involves the TOE performing application identification and policy lookups to determine what actions to take. The security policies can specify whether to block or allow a network session based on the application, the source and destination addresses, the application service (such as HTTP), users, the devices and virtual systems, and the source and destination security zones. Security zones are classified as the 'untrusted' zone, where interfaces are connected to the Internet, and the 'trusted' zone, where interfaces connect only to the internal network. Virtual systems provide a way to customize administration, networking, and security policies for the network traffic belonging to specific departments or customers. Each virtual system specifies a collection of physical and logical interfaces, and security zones for which specific policies can be tailored. Administrator accounts can be defined that are limited to the administration of a specific virtual system.

In addition, each security policy can also specify one or more security profiles, including: antivirus profiles; antispyware profiles; vulnerability protection profiles; and file blocking profiles. The profiles can identify which applications are inspected for viruses, a combination of methods to combat spyware, the level of protection against known vulnerabilities, and which type of files can be uploaded or downloaded. The TOE compares the policy rules against the incoming traffic to determine the actions to take; these actions include the following: scan for threats; block or allow traffic; logging; and packet marking. Note that this validation makes no claims regarding the efficacy of the signatures and other identification mechanisms used in these profiles; the validation only addressed the claim that the underlying tests invoked by those mechanisms are executed properly. Correct definition of the signatures and other identification mechanisms is a vendor responsibility.

The TOE also implements an information flow control policy for its VPN capability, which uses IP Security (IPSec) and Internet Key Exchange (IKE) protocols to establish secure tunnels for VPN traffic. The VPN policy makes a routing decision based on the destination IP address. If traffic is routed through a VPN tunnel, it is encrypted as VPN traffic. It is not necessary to define special rules for this policy—routing and encryption decisions are determined only by the destination IP address.

Both when the TOE 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.

The TSF relies on the domain controller in the operational environment, which is used with the User Identification Agent, to provide it with user specific information that is used in policies and reporting. Note that the User Identification Agent can only map IP addresses to users for IPv4 addresses.

3.5 Security Management

The TOE provides a number of management functions, and restricts their use to users with the appropriate privileges. The management functions include the capability to create new user accounts, configure the audit function including selection of the auditable events, configure the information flow control rules, and review the audit trail. The TOE provides Security Administrator, Audit Administrator, and Cryptographic Administrator roles. The TOE ensures the appropriate functions are restricted to these roles and there is no overlap between the roles, except that all administrators have read access to the audit trail.

The TOE offers one interface to manage its functions and access its data: a GUI management interface. The GUI management interface can be accessed via direct connection to the device, or remotely over HTTPS.

3.6 Protection of the TSF

The TOE provides fault tolerance when deployed in active/passive pairs. If the active firewall fails because a selected Ethernet link fails, or if one or more of the specified destinations cannot be reached by the active firewall, the passive firewall becomes active automatically with no loss of service. The active firewall continuously synchronizes its configuration and session information with the passive firewall over two dedicated high availability (HA) interfaces. If one HA interface fails, synchronization continues over the remaining interface.

The TOE is able to detect replay attacks and reject the data. This is true for traffic destined for the TOE itself as well as traffic passing through the TOE.

In addition, the TOE provides a set of self-tests that demonstrate correct operation of the TSF, the cryptographic functions implemented in the TSF, and the key generation components implemented in the TSF.

The TOE uses its cryptographic capabilities to secure communication between the User Identification Agent and the firewall.

3.7 Resource Utilization

The TOE is able to enforce transport-layer quotas for the number of SYN requests per second, the number of UDP packets per second that do not match an existing UDP session, and the number of ICMP packets per second.

3.8 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. The TOE can also deny establishment of an authorized user session based on location, day, and time.

3.9 Trusted Path/Channels

The TOE provides trusted paths to remote administrators accessing the TOE via HTTPS and trusted channels to authorized external IT entities.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
- Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
- The PC used for the UIA component is dedicated to this function and is not used for any other purpose.

4.1 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 augmented with ALC_FLR.2 and ATE_DPT.3).
2. This evaluation only covers the specific model numbers and software version identified in this document, and not any earlier or later versions released or in process.
3. The TOE relies on its operational environment as follows:
    a. The TOE requires the presence of a management client PC either directly connected or remotely connected to the Management port via an RJ-45 Ethernet cable. The Management port is an out-of-band management port that provides access to the GUI via HTTPS. This management client PC is part of the operational environment and is required to have a web browser (for accessing the GUI).
    b. The User Identification Agent (UIA) relies on its underlying operating system for process separation and memory protection.

c. The User Identification Agent (UIA) relies on the ability to communicate with a Microsoft Windows domain controller in the operational environment in order to provide the mapping between users and IPv4 addresses.

d. The TOE provides the capability to send the logs as SNMP traps, Syslog messages, or email notifications. This capability relies upon the presence of an SNMP, syslog, or SMTP server, as appropriate, in the operational environment. These servers are optional components that have not been subject to testing in the evaluated configuration.

4. The following product capabilities are explicitly excluded from use in the evaluated configuration:

   a. The next-generation firewall product provides an option for Central Management using the Panorama software. Panorama is a distinct product sold separately. Panorama allows management of the next-generation firewall products from a centralized management server, allowing a single management console for managing multiple devices.

   b. Command Line Interface (CLI) management via Telnet or SSH. Command Line Interface (CLI) access via SSH is restricted to the Superuser role (system admin) for maintenance and debugging purposes, which is outside normal operation of the TOE. SCP is also excluded.

   c. The UIA v3.1.2 only works with IPv4 addresses. It does not work with IPv6 addresses.

   d. HTTP web-based management.

   e. Console Port.

   f. USB Ports.

   g. Dynamic role administrator accounts. Use of the Superuser dynamic role is permitted only for initial configuration; its use must otherwise be excluded from administration of the TOE. The device administrator, device administrator (read-only), virtual system administrator, virtual system administrator (read-only), and superuser (read-only) administrator roles may not be used in the evaluated configuration

   h. Additional custom admin roles. The device comes preconfigured with three custom admin roles. One for the Security Administrator, one for the Crypto Administrator, and one for the Audit Administrator. Additional custom admin roles must not be created and used to determine access levels for administrators.

   i. Tap Mode. This is an interface mode in which traffic may only be observed and not secured.

   j. Kerberos for authentication of administrators.

   k. Custom Applications and custom definition methods, which are used by Administrators to define custom applications in order to identify and control their own internally developed applications.

   l. Use of NTP to synchronize the system's time. Time must be defined locally.

   m. Captive Portal, which provides the capability to identify users when they do not authenticate to Active Directory.

n. GlobalProtect, a VPN capability for remote users. This is a separately licensed feature.

o. HIP Profiles. This is part of the GlobalProtect feature set used to verify the host's configuration prior to granting access.

p. SSL-VPN, a VPN capability for remote users.

q. Terminal Services Agent. This is a separate software image used when terminal services are required along with user identification

r. REST API, an API used to perform select configuration and administration tasks on the firewall. The REST API is available only to administrators with Superuser accounts and is therefore not permitted in Common Criteria mode.

s. User-ID XML API, an API used to provide user to IP mappings to the firewall.

t. Log Forwarding using FTP and TFTP.

u. RADIUS for authentication of administrators.

v. SSHv1. This is disabled in Common Criteria mode.

w. Authentication methods (e.g., CHAP/PAP) used for PPPoE.

x. eDirectory.

y. Tunnel monitoring.

z. SSLv1, SSLv2, SSLv3. These are disabled in Common Criteria mode.

aa. DNS. This is not required to enforce any SFRs. The "U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments" states in section 2.3: "Remote administration is a required information flow to the TOE, authentication/certificate servers, Network Time Protocol (NTP) servers, as well as any other IT entities are optional."

bb. Software Update. The TOE system software must not be updated in order to maintain CC compliance.

cc. Active/active HA pairs.

dd. Botnet.

ee. Country based policy enforcement.

5. The following capabilities, although not explicitly excluded, have not been subject to evaluation and so no claims are made as to their efficacy:

    a. The efficacy of pre-defined anti-virus, anti-spyware, and vulnerabilities profiles; file identification and application identification schemes are not covered by the evaluation.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and design documentation.

5.1 TOE Architecture

The TOE's architecture is divided into three subsystems: the control plane, the data plane and the User Identification Agent. The *control plane* provides system management functionality while the *data plane* handles all data processing on the network; both reside on the firewall appliance. The *User Identification Agent* is installed on a separate PC on the network and communicates with the domain controller to retrieve user-specific information. It allows the next-generation firewall to automatically collect user information and include it in policies and reporting.

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

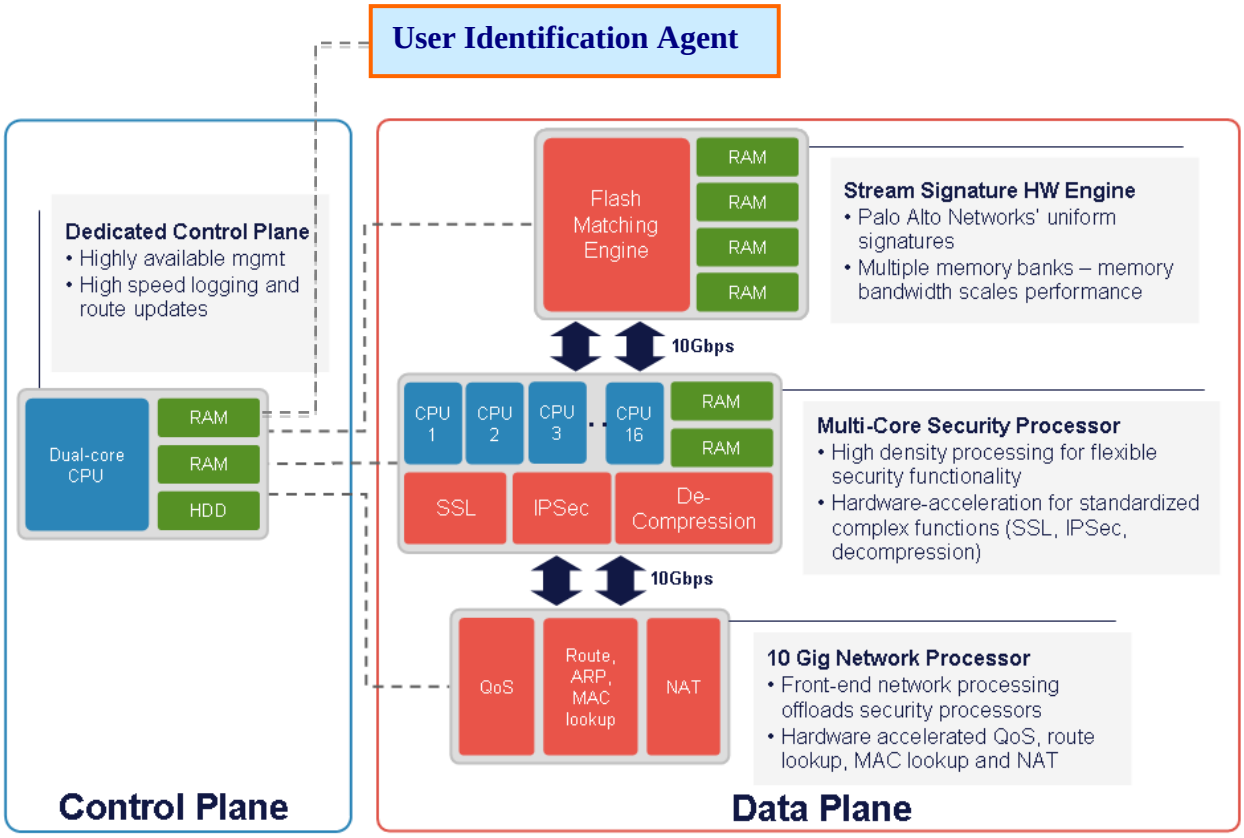

Figure 1. Hardware and Software Architecture of the PA Next-Generation Firewalls

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 (Flash Matching Engine), each with its own dedicated memory and hardware processing.

5.1.1 Control Plane

The control plane provides all device management functionality, including the following:

- All management interfaces: CLI (direct console access— used for maintenance, recovery and debugging purposes, which is outside the normal operation of the TOE.), GUI interface, syslog logging, SNMP, and ICMP.
- 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 (reporting is excluded from the evaluated configuration).
- 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 used for policy enforcement.

5.1.2 Data Plane

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

- 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 TOE'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). The certificates used by the TOE during forward proxying include as much relevant data from the external server's original certificate as possible (i.e., validity dates, certificate purpose, common name, and subject information). For inbound connections (external client to internal server), the TOE can decrypt incoming traffic and control the traffic within the SSL tunnel. SSL decryption is configured as a rulebase in which match criteria include zone, IP address, and User-ID. SSL proxy is configured by creating a Certificate Authority certificate (CA cert) on the firewall. When a client attempts to connect with a remote server, if a decryption policy is matched, the firewall will create a connection with the server and another connection with the client, inserting itself in the middle.

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 the any port forwarding is detected, the application becomes an SSH-tunnel, and based on the policy, the session might get denied.

5.1.3 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 XP with SP2 (or higher than SP2), Windows Vista, 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, which uses it for policy enforcement and reporting. The UIA maintains mapping information received from the Domain Controller, which it synchronizes to the firewall table. The UIA works only with IPv4 addresses; IPv6 addresses are not supported.

5.1.4 Management Interfaces

In the evaluated configuration, the TOE can be managed by a computer either directly connected or remotely connected to the Management port via an RJ-45 Ethernet cable. The Management port is an out-of-band management port that provides access to the GUI via HTTPS. The management computer is part of the operational environment and required to have a web browser (for accessing the GUI).

6 Evaluation Evidence

This section provides a list of the evaluation evidence issued by the developer (and sponsor). Documents that are publicly available to customers via the Palo Alto Networks support web site are indicated with *; documents that are not publicly available are indicated with †.

6.1 Guidance documentation

The publicly available guidance documentation examined during the course of the evaluation is as follows:

- *Palo Alto Networks Next-Generation Firewall Common Criteria Evaluated Configuration Guide, Version 2.0, April 26, 2013**
- *Palo Alto Networks Administrator's Guide Release 4.0, Part Number 810-000061-00A**
- *PAN-OS Command Line Interface Reference Guide Release 4.0, Part Number 810-000065-00A**
- *PA-500 Series Hardware Reference Guide, Part Number 810-000036-00C**
- *PA-500 Quickstart guide, Part Number 810-000041-00A**
- *PA-2000 Series Hardware Reference Guide, Part Number 810-000019-00F**
- *PA-2000 Quickstart Guide, Part Number Part Number 810-000018-00A**
- *PA-4000 Series Hardware Reference Guide, Part Number 810-000002-00H**
- *PA-4000 Quickstart Guide, Part Number 810-000001 rev 00D**
- *PA-5000 Series Hardware Reference Guide, Part Number 810-000056-00A**
- *PA-5000 Quickstart Guide, Part Number 810-000058 rev 00A**

6.2 Design documentation

- *Security Architecture Palo Alto Networks Inc. PA-Series Firewall, Document Version 1.5, February 8, 2013†*
- *Functional Specification Palo Alto Networks Inc. PA-Series Firewall, Document Version 1.11, April 4, 2013†*
- *TOE Design Palo Alto Networks Inc. PA-Series Firewall, Document Version 1.14, April 4, 2013†*

6.3 Lifecycle documentation

- *Palo Alto Networks Inc. PA-Series Firewall Secure Delivery Processes and Procedures, Version 1.5, April 4, 2013†*
- *Palo Alto Networks Inc. PA-Series Firewall Development Security Measures, Version 1.4, April 4, 2013†*
- *Palo Alto Networks Inc. PA-Series Firewall Life-Cycle Development Process, Version 1.3, September 12, 2012†*
- *Palo Alto Networks Inc. PA-Series Firewall Configuration Management Processes and Procedures, Version 1.7, April 5, 2013†*
- *Palo Alto Networks Inc. PA-Series Firewall Flaw Remediation, Version 1.2, September 10, 2012†*

6.4 Test documentation

- *Test Plan and Functional Test Coverage/Depth – Part 1, Version 1.8, April 5, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 2a, Version 1.7, April 5, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 2b, Version 1.5, February 6, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 3, Version 1.6, February 25, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 4, Version 1.7, February 25, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 5, Version 1.6, April 5, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 6, Version 1.8, March 1, 2013†*
- *Test Plan and Functional Test Coverage/Depth – Part 7, Version 1.1, February 26, 2013†*
- *PAN Test Case Coverage v1.1, 5 April 2013†*
- *IPv6-L2-L3-2 – samples.xls, February 1, 2013†*
- *Boundary Tests Examples.docx, January 31, 2013†*
- *PAN Capacity Testing - one test from each class.docx, February 1, 2013†*
- *IPv6-L2-L3-SFR-mapping.xls, April 5, 2013†*

- *UID test with DC.docx, April 5, 2013†*

6.5 Security Target

- *Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series, PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2 Security Target, Version 1.0, April 11, 2013*

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2.

Evaluation team testing was conducted at the vendor's development site February 18-22, 2013.

7.1 Developer Testing

The vendor's test philosophy involves the use of manual test procedures that are based primarily on testing the claimed security functions of the TOE as represented by the SFRs specified in the ST. Essentially, Palo Alto developed a set of test cases that correspond to security functions claimed in the ST, ensuring that all security functions presented at the external interfaces are tested and that all TSFI, subsystems and modules are tested.

Test cases are performed using the Web interface, the CLI, and some third party testing tools. The CLI is excluded from use in the actual evaluated configuration except for maintenance and debugging purposes. It is used in the developer's testing as a test tool primarily for convenience and test setup purposes. The Web interface, on the other hand, is fully tested such that the test cases demonstrate that it fully answers the admin-related SFRs. The tests consist of both positive and negative testing.

The Palo Alto Test Plan and Functional Test Coverage/Depth Part 1 document includes an introduction, test approach, test environment and test evidence organization section. The test environment description includes diagrams of the test network configuration and all components used in testing. This section also provides some basic information regarding the standard configuration and setup, which includes installing the TOE in CC mode, creating TOE security roles and creating configuration files for testing purposes. Section 3.3 of the Test Plan provides a table that lists and describes each test case. Test Cases are grouped into a number of separate documents that are identified by their part number (as listed in Section 6.4). The Test Plan also provides mappings of SFRs, TSFI and Subsystems and Modules to test cases.

The Test Plan includes a table that identifies the tests that will be covered by source code review during onsite testing and also provides a brief rationale for why these could not be reasonably tested otherwise. Lastly, the Test Plan includes another table identifying the test case format. Each test case is mapped to the appropriate SFR(s), TSFI, Subsystems and Modules and includes the Test Case identifier, Test case description/goal, Test Setup, Test Steps, Expected Results, Actual Results, Cleanup, Date Tested and Overall Pass/Fail status.

The evaluation team found that the test documentation maps the test cases to the TOE security behaviors identified in the functional specification and TOE design and to the TOE security

functional requirements. The evaluation team confirmed the mapping and found that the correspondence between the test documentation and the design documentation is accurate.

7.2 Evaluation Team Independent Testing

The evaluation team exercised the developer and independent tests against the evaluated configuration of the TOE.

The vendor has run all vendor tests across the following four platforms: PA-500, PA-2050, PA-4050 and PA-5060 with the User Identification Agent installed on Windows XP. The User Identification Agent binary image is the same for all versions of Windows. The actual results collected are shown for only one platform when the results are exactly the same on all four platforms. All security-relevant code (including all audit functionality) is shared amongst all of the devices. The devices differ only in capacities, performance, and physical configuration.

The majority of the vendor test cases utilize the Virtual Wire networking configuration mode. This is sufficient because the TOE software that applies information flow security policies is independent of the part that determines packet flow, therefore, a security policy could be configured to block a particular IP address, port, and application in any of the networking modes and it would look exactly the same.

The evaluation team ran a sample of the vendor test suites across three of the claimed appliances (PA-2020, PA-4060 and PA-5050) running PAN-OS v4.0.12-h2 and including the User Identification Agent v3.1.2 installed on a Windows PC. The chosen sample represented approximately 20% of the vendor test suite and was determined based on the following factors:

- The test subset covers all of the TSFI (GUI, Network Interfaces, User Identification Agent), subsystems and modules.
- The test subset covers all security functions claimed in the ST.
- The test subset covers all vendor tests subject to source code review as listed in Section 4 of the vendor's Test Plan. (Note these test cases are listed here, but are considered part of the evaluation team testing and the results will be described in Appendix B).
- The test subset covers IPv6 testing.

The following hardware was used to create the test configurations:

- PA-2020, PA-4060, PA-5020, PA-5050, and PA-5060 appliances running PAN-OS v4.0.12-h2, with User Identification Agent, v3.1.2.
- User Identification Agent on a Windows machine.
- Domain Controller.
- Linux Server machines running Wireshark and OpenSSL s_client software.
- Ethernet router, Cat 5e cabling, and any other items required to create a functional Ethernet network environment.

The following software (including tools used in the vendor tests) was installed on the machines used for the tests:

- PAN-OS v4.0.12-h2
- User Identification Agent v3.1.2
- Linux

- Windows
- WS_FTP
- Putty
- Active Directory
- Test Tools:
    - nping
    - tcpsic (custom)
    - udpsic (custom)
    - Wireshark
    - Tcpreplay
    - iReasoning MIB Browser
    - VNC Server

The evaluation team performed the following additional functional tests:

- **Auditable Events**. The evaluation team confirmed that modifying aspects of a user such as user role and password is audited. Additionally, the evaluation team verified that the startup and shutdown of the appliance is audited.
- **Audible Alarm.** The evaluation team confirmed that the TOE can be configured to generate an audible alarm upon meeting one of the failure thresholds chosen by the evaluator (e.g. login failure).
- **Account Lockout**. The evaluation team confirmed that the TOE can detect when an administrator configurable number of failed login attempts has occurred and will perform the configured failed login action which can be one of the following:
    - Lock the account for a configured Lockout period
    - Lock the account until a Security Administrator unlocks it
- **Password Structure Criteria.** The evaluation team confirmed that the TOE enforces a minimum password length of 6 characters and a maximum password length of 15 characters. Additionally, the team verified that passwords can be composed of 95 possible characters (including space).
- **CLI Role Restriction.** The evaluation team confirmed that SSH Admin Console (CLI) access is restricted to the Superuser account and that the TOE security roles cannot access the TOE via this interface. Additionally, the team verified that the SSH Admin Console can be disabled. The CLI is excluded from normal operational use in the evaluated configuration and is only accessed by the superuser account for maintenance and debugging purposes.
- **Configuration File Modification**. The evaluation team confirmed that the audit and configuration file data cannot be directly accessed from the GUI management interfaces which do not provide the capability to traverse the directory structure of the underlying operating system.
- **URL Filtering Profiles**. The evaluation team confirmed the TOE's ability to define a URL Filtering Profile including definition of a block list, an allow list and the use of

wildcard patterns. The team verified that access to web sites listed on the block list will be blocked, while access to web sites on the allow list will be allowed.

- **FIPS Encryption**. The evaluation team confirmed that the TOE did not provide any means of requesting other encryption algorithms when the TOE is in FIPS mode.
- **User Identification Agent IPv6**. The evaluation team confirmed that the UIA does not support IPv6 addresses and will not accept User ID to IPv6 address mappings.
- **Reliable Time**. The evaluation team confirmed the consistency of timestamps documented in the audit log when user login is performed via the GUI.
- **Revoked User**. The evaluation team determined that when a user account is deleted or the password is changed, the appliance must be rebooted in order for the revocation to take place immediately.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE. While there were a few older vulnerabilities that came up in the search, none of them were found to be related to the TOE version and/or they were related to functionality that is excluded in the TOE. In each case, the evaluation team confirmed with the vendor that there were bug fixes that had been applied as a result of the TOE's flaw remediation procedures being exercised. The evaluation team also considered the open source products used in the TOE. The team determined, through analysis of vulnerability descriptions, consideration of the method of use of the TOE, and the TOE's flaw remediation procedures that none of the reported vulnerabilities were applicable to the TOE.

In addition to the open source search, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities. The evaluation team performed the following vulnerability tests:

- **Web Vulnerability Scan**: The evaluation team performed a web vulnerability scan and confirmed that the TOEs web browser GUI does not subject the system to any web application security flaws (OWASP Top Ten), such as cross site scripting (XSS), broken authentication and session management, failure to restrict URL access, etc.
- **Port and Protocol Scan**: The evaluation team confirmed that all only open ports and services needed by the TOE were identified by the scan.
- **Invalid Parameter Handling**: The evaluation team performed fuzz testing to determine how the TOE handles malformed packets. The team verified that the TOE remains functional and operates as normal after malformed packets were dropped or discarded by the TOE. More importantly, it was observed that the TOE did not crash or fail insecure (e.g., allow all information flow to pass through the TOE).
- **Content Updates**: The evaluation team verified that content updates are downloaded over a secure connection using HTTPS (HTTP over TLS).
- **User Account Harvesting**: The evaluation team verified that the TOE authentication mechanism returns the same error message for incorrect username or incorrect password to ensure that the TOE is not vulnerable to attackers gathering user accounts.

- **User Input Validation:** The evaluation team verified that attempts to enter scripts and other invalid data into various fields in the GUI were unsuccessful and resulted in appropriate error messages being generated by the TOE in each case.
- **Web Proxy Manipulation**: The evaluation team verified that the GUI interfaces are not vulnerable to web attribute manipulation by relying on the client-side syntax checking.
- **Denial of Service**: The evaluation team confirmed that the TOE is not susceptible to a denial of service attack via a flood of packets on TCP port 443.
- **ICMP**: The evaluation team confirmed that when ping is enabled on the management interface, the TOE is not susceptible to well-known ICMP attacks.

8 Evaluated Configuration

The evaluated version of the TOE is identified as the Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall which includes the models PA-500, PA-2020, PA-2050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060 appliances running PAN-OS software version 4.0.12-h2 and including the User Identification Agent client version 3.1.2.

The TOE consists of the following components:

- **Hardware appliance**. This includes the physical port connections on the outside of the appliance cabinet, an internal hardware cryptographic module used for the cryptographic operations provided by the TOE, and a time clock that provides the time stamp used for the audit records.
- **PAN-OS version 4.0.12-h2**. The firmware component that runs the appliance. PAN-OS is built on top of a Linux kernel and runs along with Appweb (the web server that Palo Alto Networks uses), crond, syslogd, and various vendor-developed applications that implement PAN-OS capabilities. PAN-OS provides the logical interfaces for network traffic. PAN-OS runs on both the Control Plane and the Data Plane and provides all firewall functionalities provided by the TOE, including the threat prevention capabilities as well as the identification and authentication of users and the management functions. PAN-OS provides unique functionality on the two planes based on the applications that are executing. The Control Plane provides a GUI Web management interface to access and manage the TOE functions and data. The Data Plane provides the external interface between the TOE and the external network to monitor network traffic so that the TSF can enforce the TSF security policy.
- **User Identification Agent (UIA) version 3.1.2**. This is the client software program installed on one or more PCs on the protected network. The UIA provides the firewall with the capability to automatically collect user-specific information that is used in security policy enforcement and reporting.

The physical boundary of the TOE comprises the firewall appliance (PA-500, PA-2020, PA-2050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060), together with the User Identification Agent (UIA) component. The nine models of the next-generation firewall differ in their performance capability, but they provide the same security functionality, with the exception of virtual systems, which are supported by default (without an additional license) on the PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060. The PA-2000 Series can support virtual systems with the purchase of an additional license. The PA-500 cannot support virtual systems.

Virtual systems specify a collection of physical and logical firewall interfaces that should be isolated. Each virtual system contains its own security policy and its own set of logs that will be kept separate from all other virtual systems.

The firewall appliance attaches to a physical network. Models differ by the number and types of ports supported, as follows:

- **PA-500**: 8 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)
- **PA-2020**: 12 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 2 Small Form-Factor Pluggable (SFP) Gbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)
- **PA-2050**: 16 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 4 Small Form-Factor Pluggable (SFP) Gbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)
- **PA-4020/4050**: 16 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 8 Small Form-Factor Pluggable (GFP) Mbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); 1 DB-9 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization
- **PA-4060**: 4 XFP 10 Gbps ports for management traffic; 4 Small Form-Factor Pluggable (SFP) Mbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); 1 DB-9 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization
- **PA-5020**: 12 RJ-45 10/100/1000 ports for network traffic. 8 Small Form-Factor Pluggable (SFP) ports for network traffic. One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two RJ-45 ports for high-availability (HA) control and synchronization.
- **PA-5050**: 12 RJ-45 10/100/1000 ports for network traffic. Eight Small Form-Factor Pluggable (SFP) ports for network traffic. Four SFP+ ports for network traffic. One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two RJ-45 ports for high-availability (HA) control and synchronization.
- **PA-5060**: 12 RJ-45 10/100/1000 ports for network traffic. Eight Small Form-Factor Pluggable (SFP) ports for network traffic. Four SFP+ ports for network traffic. One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two RJ-45 ports for high-availability (HA) control and synchronization.

In the evaluated configuration, the TOE is managed bya computer either directly connected or remotely connected to the Management port via an RJ-45 Ethernet cable. The Management port is an out-of-band management port that provides access to the GUI via HTTPS. The computer is part of the operational environment and required to have a web browser (for accessing the GUI).

Traffic logs, which record information about each traffic flow or problems with the network traffic, are logged locally by default. However, the TOE offers the capability to send the logs as SNMP traps, Syslog messages, or email notifications. This capability relies on the operational environment to include the appropriate SNMP, syslog or SMTP servers. These servers are optional components, which have not been subject to testing in the evaluated configuration.

The operational environment includes a domain controller to be used with the User Identification Agent. The User Identification Agent itself is installed on one or more PCs in the operational environment, and is supported on Windows XP with SP2 (or higher than SP2), Windows Vista, Windows Server 2003 (32-bit) with SP2 (or higher), or Windows Server 2008 (32-bit and 64-bit). The operational environment also includes an SNMP client.

The port for connecting a serial console (DB-9 in PA-4000 series and RJ-45 for PA-500, PA-2000 and PA-5000 series) is not part of the TOE evaluated configuration, as it is enabled only for output in Common Criteria mode.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 2 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 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 agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL4 augmented with ALC_FLR.2 and ATE_DPT.3" certificate rating be issued for Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2.

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

Table 2. TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
ALC_CMC.4	Product support, acceptance, procedures and automation
ALC_CMS.4	Problem tracking CM coverage

Assurance Component ID	Assurance Component Name
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_FLR.2	Flaw reporting procedures
ALC_LCD.1	Developer defined life- cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.3	Focused vulnerability analysis

10 Validator Comments/Recommendations

1. This evaluation does not cover the efficacy or completeness of anti-virus signatures, anti-spyware signatures, vulnerability signatures or App-ID. It only provides confirmation that these mechanisms operate properly.
2. The TOE enforces a minimum password length of 6 and a maximum password length of 15. While the TOE does not provide a mechanism to enforce password complexity, the Palo Alto Networks Next-Generation Firewall Common Criteria Evaluated Configuration Guide provides password complexity requirements for the evaluated configuration.
3. A support service account is required for an additional service fee in order to obtain information about bug fixes included in the release notes.
4. While the TOE's ability to manage session identifiers has not been formally assessed against NIST SP 800-53 Revision 3 SC-23 (Session Authenticity), the vendor confirms that the TOE meets SC-23(2), SC-23(3), SC-23(4) and SC-23(5).
5. The underlying operating system of the TOE is a general-purpose operating system that has been hardened for security purposes. The vendor has not formally assessed the operating system against the corresponding DISA implementation guide. Although there appear to be some requirements that are not met, the vendor has confirmed that key operating system files are protected. The evaluation team has considered the vendor's analysis during their vulnerability testing. This analysis did not identify any residual risk resulting from the hardened operating system configuration.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is *Palo Alto Networks PA-500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2 Security Target, Version 1.0, April 11, 2013*.

13 Acronyms and Abbreviations

API	Applications Programming Interface
CA	California
CA	Certificate Authority
Cat 5	Category 5
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Test Laboratory
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria and Common Methodology for IT Security Evaluation
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DISA	Defense Information Systems Agency
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
Gbps	Giga Bits-per-second
GUI	Graphical User Interface
HA	High Availability
HIP	Host Identity Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
IT	Information Technology
Mbps	Mega Bits-per-second
MD	Maryland
MIB	Management Information Base
MRPP	U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OWASP	Open Web Application Security Project
PA	Palo Alto
PAP	Password Authentication Protocol
PC	Personal Computer

PP	Protection Profile
PPPoE	Point-to-Point Protocol over Ethernet
RADIUS	Remote Authentication Dial In User Service
REST	Representational State Transfer
RJ	Registered Jack
SAIC	Science Applications International Corporation
SC	NIST SP 800-53 Family: System and Communications Protection
SFP	Security Function Policy
SFP	Small Form-Factor Pluggable
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
ST	Security Target
SYN	Synchronise packet in transmission control protocol (TCP)
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TSF Interface
U.S.	United States
UDP	User Datagram Protocol
UIA	User Identification Agent
URL	Uniform Resource Locator
USB	Universal Serial Bus
VNC	Virtual Network Computing
VPN	Virtual Private Network
VR	Validation Report
XML	Extensible Markup Language
XP	Version of Microsoft Windows
XSS	Cross Site Scripting

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006, CCIMB-2006-09-001.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-003.

[4] Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004.

[5] Palo Alto Networks PA_500, PA-2000 Series, PA-4000 Series and PA-5000 Series Next-Generation Firewall running PAN-OS 4.0.12-h2 Security Target, Version 1.0, April 11, 2013.