National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall

Report Number:	**CCEVS-VR-VID10330-2011**
Dated:	**17 October 2011**
Version:	**0.2**

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

Rick Murphy

Noblis
Falls Church, VA

Common Criteria Testing Laboratory

SAIC
Columbia, MD

Table of Contents

List of Tables

1. Executive Summary

The evaluation of the Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall 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 October 2011. 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 2 augmented with ALC_FLR.2. The information in this Validation Report is largely derived 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-2000 Series and PA-4000 Series Firewall devices comprising model appliances PA-2020, PA-2050, PA-4020, PA-4050, and PA-4060 running PAN-OS software version 2.1.7. The TOE also includes the User Identification Agent client version 2.1.4

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 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 automatically collect user-specific information that it uses in policies and reporting.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall Security Target (ST).

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

1.1. Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	The Target of Evaluation (TOE) is Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall devices comprising: • The model appliances PA-2020, PA-2050, PA-4020, PA-4050, and PA-4060 running PAN-OS software version 2.1.7 • The TOE also includes the User Identification Agent client version 2.1.4
Sponsor:	**Palo Alto Networks Inc.** 3300 Olcott St Santa Clara, CA 95054

VALIDATION REPORT
Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall

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:

24 April 2009

Completion Date:

15 November 2011

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 2 augmented with ALC_FLR.2

Description:

The PA-2000 Series and PA-4000 Series firewalls 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 automatically collect user-specific information that it uses in policies and reporting.

Disclaimer:

The information contained in this Validation Report is not an endorsement of the Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall devices product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

PP:

US Government Protection Profile for Traffic-Filter firewall in Basic Robustness Environments Version 1.1, July 25, 2007.

Evaluation Personnel:

Science Applications International Corporation:
Katie Sykes
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:

- An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
- An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
- An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
- An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
- An unauthorized person may send impermissible information through the TOE that results in the exploitation of resources on the internal network.
- Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
- Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
- An unauthorized person may read, modify, or destroy security critical TOE configuration data.
- An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
- The TOE may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons.

2. Identification

The evaluated product is **Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall** comprising:

- The model appliances PA-2020, PA-2050, PA-4020, PA-4050, and PA-4060 running PAN-OS software version 2.1.7
- The User Identification Agent client version 2.1.4

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-2000 Series and PA-4000 Series Firewall devices security policy has been extracted and reworked from the Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall ST 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). Both the management GUI and the CLI are used to review the audit trail. The management GUI offers options to sort and search the audit records. The TOE stores the audit trail and protects it. The TOE protects the audit trail by providing only restricted access to it; by not providing interfaces to modify the audit records, and by ensuring that no new audit records are lost if the audit trail becomes full. The TOE provides the capability to manually archive log files and securely export them using Secure Copy (SCP). The TOE also provides a time-stamp for the audit records.

3.2. Identification and Authentication

The TOE ensures that all users accessing the TOE user interfaces are identified and authenticated. The TOE maintains information that includes username, password, virtual system(s) and role (set of privileges) that it uses to authenticate the human user and associate him/her to a role. The TOE also provides a mechanism to lock out user accounts when an administrator-configured number of consecutive unsuccessful login attempts have been made. The TOE can be configured to unlock affected accounts after a configurable period of time or to maintain the account lockout until an administrator unlocks the account.

3.3. User Data Protection

The TOE enforces an information flow control SFP to control the type of information that is allowed to flow through the TOE. The enforcement process involves the TOE performing application identification and policy lookups to determine what actions to take. The security policies 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. A security zone, or multiple security zones, are defined and configured as needed to specify the desired security policy. A security zone is classified either as an ‘untrusted’ zone where interfaces are connected to the Internet (or outside network), or as a ‘trusted’ zone where interfaces connect only to the internal network. The 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 the applications that are inspected for viruses, a combination of methods to combat spyware, and the level of protection against known vulnerabilities[1]. The TOE compares the policy rules against the incoming traffic to determine what actions to take including: scan for threats, block or allow traffic, logging, and packet marking.

The TOE includes cryptographic mechanisms[2] used for SSL forward proxy to decrypt SSL traffic and apply policy rules before re-encrypting it to its destination. The TOE also provides a method to decrypt incoming SSL traffic and apply policy rules when protecting servers.

[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 correctness of the cryptographic requirements in the Security Target is ascertained by vendor assertion.

3.4. Security Management

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, including allowing users to change their own passwords, configure the audit function, configure the information flow control rules, and review the audit trail. The TOE offers two interfaces to manage its functions and access its data—a text-based CLI and a GUI management interface. Both the CLI and GUI are accessed via direct connection to the device.

3.5. Protection of the TSF

The TOE provides fault tolerance, when it is 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 uses SSLv3 to secure communication between the User Identification Agent and the firewall.

4. Assumptions

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

- The PC used for the UIA component is dedicated to this function and is not used for any other purpose.
- The TOE is physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The TOE does not host public data.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- Information cannot flow among the internal and external networks unless it passes through the TOE.
- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
- All human users including the authorized administrators cannot access the TOE remotely from the internal or external networks.
- Authorized administrators may not access the TOE remotely from the internal and external networks.
- It is assumed a VT-100 terminal, or a device that correctly emulates a VT-100 terminal, is available in the operational environment for use as a locally connected console.

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 2 augmented with ALC_FLR.2).
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 for the following components and capabilities:
    a. A VT-100 terminal, or device able to emulate a VT-100 terminal, connected via the serial console port, to support local management of the TOE via the CLI.

    b. A management client PC, directly connected to the Management port via an RJ-45 Ethernet cable (i.e., with no intervening network infrastructure). The Management port is an out-of-band management port that provides access to the GUI via HTTPS and to the CLI via SSH. The computer is part of the operational environment and required to have a web browser for accessing the GUI (IE version 5.5 and later, and Firefox 1.0 and later are supported) or an SSH client for accessing the CLI.

    c. The User Identification Agent (UIA) relies on its underlying operating system for process separation and memory protection.

    d. The capability provided by the UIA relies on its being able to communicate with a Microsoft Windows domain controller in the operational environment.

    e. The TOE provides the capability to send the logs as SNMP traps, Syslog messages, or email notifications. This capability requires the presence of an SNMP, syslog, or SMTP server, as appropriate, in the operational environment.
4. The following capabilities are explicitly excluded from use in the evaluated configuration:
    a. The PA-2000 Series and PA-4000 Series firewall product has the capability to support remote administration of the TOE using the CLI over Telnet or SSH and the GUI over HTTP or HTTPS. Support for remote administration is disabled and is not included in the evaluated configuration. In accordance with PD-0146, the ST explicitly disallows the use of remote administration because the cryptographic mechanism used to secure the remote administration traffic is not FIPS validated. Note that the use of cryptography to analyze traffic flow is still included in the evaluated configuration as the PP does not require that this mechanism be FIPS certified.

    b. The use of Telnet and HTTP to access the TOE's management interfaces from the PC directly connected to the Management port is excluded from the evaluated configuration.

    c. The deployment of the TOE in Tap Mode is excluded from the evaluated configuration.

    d. The use of a RADIUS server and Captive Portal are not supported in the evaluated configuration.

    e. The PA-2000 Series and PA-4000 Series firewall product provides an option for Central Management using the Panorama software. This capability is not included in the scope of evaluation. Panorama is a separate product and is sold separately. Panorama allows the firewall products to be managed from a centralized management server, allowing a single management console for managing multiple devices.

    f. The use of the Trivial File Transfer Protocol (TFTP) to transfer files from the TOE to another IT entity is excluded from the evaluated configuration.

g. The use of Telnet to connect from the TOE to another IT entity is excluded from the evaluated configuration.

h. The use of Custom Role-Based Administration is excluded from the evaluated configuration. Only the default administrative roles provided with the TOE are to be used in the evaluated configuration.

i. The ability to download and install an update of the TOE software from the management interface is excluded from the evaluated configuration.

j. The PA-2000 Series and PA-4000 Series firewall product provides IPSec VPN capabilities that are not included in the evaluated configuration. The VPN functionality is excluded in accordance with PD-0148 and because the cryptographic mechanism that implements it is not FIPS certified.

k. The TOE's ability to allow remote technical support from the Palo Alto Technical Assistance Center (PA TAC) to login to the TOE is excluded from the evaluated configuration.

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. While the capability for the administrator to install updates to application definitions and threat signatures has been evaluated, the quality and efficacy of such application definitions and threat signatures has not.

   b. Note that while the Log forwarding functionality is included in the product and can be used in the evaluated configuration, it has not been subject to evaluation.

   c. The use of an external NTP server is allowed in the evaluated configuration, but has not been subject to evaluation.

   d. The ability to SSH from the CLI to an external IT entity is not excluded from the evaluated configuration, but has not been subject to evaluation.

   e. The TOE's data filtering capability, which allows the administrator to define security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall, has not been subject to evaluation.

   f. The TOE's ability for administrators to create definitions for applications that are not recognized by the TOE has not been subject to evaluation.

   g. While the ability of the TOE to identify an application and enforce policy based on that identification has been tested, no claims about the completeness or efficacy of application identification are made.

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.

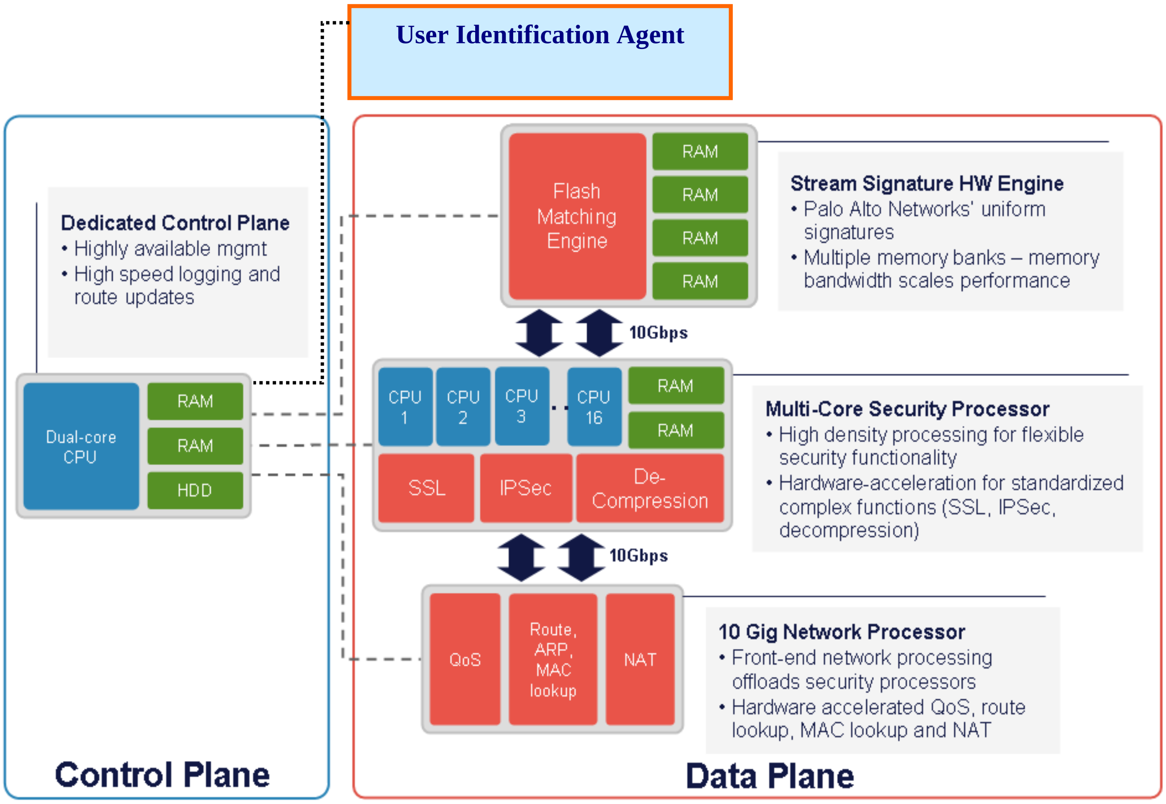
5.1. TOE Architecture

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[3] on the network and communicates with the domain controller to retrieve user-specific information, such as users, user groups, and machines deployed in the domain, and

[3] It is usually sufficient to install the User Identification Agent on a single PC in the domain.

make this information available to the firewall appliance. Specifically, the User Identification Agent returns the user-specific information it collects from the domain controller to the control plane, which then provides it to the data plane to use to make policy decisions on rules based on the user. This capability enables the firewall appliance to include collected user information in policies and reports.

The following diagram depicts both the hardware and software architecture of the PA-2000 Series and PA-4000 Series firewall.


User Identification Agent
Dedicated Control Plane
• Highly available mgmt
• High speed logging and route updates
Dual-core CPU
RAM
RAM
HDD
Control Plane
Flash Matching Engine
RAM
RAM
RAM
RAM
Stream Signature HW Engine
• Palo Alto Networks' uniform signatures
• Multiple memory banks – memory bandwidth scales performance
10Gbps
CPU 1
CPU 2
CPU 3
CPU 16
RAM
RAM
SSL
IPSec
De-Compression
Multi-Core Security Processor
• High density processing for flexible security functionality
• Hardware-acceleration for standardized complex functions (SSL, IPSec, decompression)
10Gbps
QoS
Route, ARP, MAC lookup
NAT
10 Gig Network Processor
• Front-end network processing offloads security processors
• Hardware accelerated QoS, route lookup, MAC lookup and NAT
Data Plane

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.

Control Plane

The control plane provides all device management functionality, including:

- All management interfaces: CLI (direct console access), 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, configuration, and system logs. All logs are stored locally and can also be exported to external IT systems as SNMP traps, syslog messages, or email notifications
- 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

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
- URL filtering for web browsing
- Application decoding, threat scanning for all recognized types of threats and threat prevention
- Logging, with all logs sent to the control plane for processing and storage

IPsec VPNs are a capability of the product, but are not supported by the TOE.

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). 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.

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 service pack 2 or higher and Windows Server 2003 with service pack 2 or higher. The agent communicates with a Microsoft Windows Domain Controller to obtain user information (such as user groups, users, and machines deployed on the domain controller) and makes the information available to the firewall. The firewall includes this information it in policies and reporting.

Management Interfaces

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

- A directly-connected console (i.e., connected to the Console port), which must be a VT-100 terminal or a device that can emulate a VT-100 terminal. This provides direct access to the CLI. The console is part of the operational environment and is expected to correctly display what is sent to it from the TOE.
- A computer directly connected to the Management port via an RJ-45 Ethernet cable (i.e., with no intervening network infrastructure). The Management port is an out-of-band management port that provides access to the GUI via HTTPS and to the CLI via SSH. The computer is part of the operational environment and required to have a web browser (for accessing the GUI) or SSH client (for accessing the CLI).

6. Evaluation Evidence

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor). Much of this evidence is proprietary and not available outside the evaluation; proprietary documents are indicated with ‡.

6.1. Guidance documentation

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

Document	***Version***	***Date***
Palo Alto Networks Administrator's Guide, Release 2.1.7 (includes Appendix D with Common Criteria evaluated configuration guidance)		
PAN-OS Command Line Interface Reference Guide, Release 2.1		
PA 4000 Series Hardware Reference Guide, Revision F (4050, 4020 and 4060 models)		
PA 2000 Series Hardware Reference Guide, Revision E (2020 and 2050 models)		
PA-2000 Series QuickStart Guide, Part Number 810-000018-00A		
PA-4000 Series QuickStart Guide, Part Number 810-000001-00D		

6.2. Design documentation

Document	***Version***	***Date***
Security Architecture‡	*Doc 3423, Version 3*	*October 6, 2011*
Functional Specification‡	*Doc 3419, Version 3*	*October 17, 2011*
TOE Design‡	*Doc 3420, Version 3*	*October 6, 2011*

6.3. Lifecycle documentation

Document	***Version***	***Date***
EAL2 Life-Cycle Support Documentation‡	*Doc 3422, Version 3*	*October 18, 2011*
Flaw Remediation Procedures‡	*Doc 2190, Version 2*	*September 2011*

6.4. Test documentation

Document	***Version***	***Date***
Test Plan and Procedures‡	*Doc 3421, Version 3*	*October 17, 2011*

6.5. Security Target

Document	***Version***	***Date***
Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall Security Target	*Version 1.0*	*October 18, 2011*

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-2000 Series and PA-4000 Series Firewall.

Evaluation team testing was conducted at the vendor's development site August 22 through August 25, 2011.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1. Developer Testing

The vendor's test philosophy involves the use of manual test procedures that are primarily based 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 are tested.

The tests are performed both via the dedicated management port for the web interface and through the console port for the CLI. The test plan and test cases also rely on third party testing tools. The tests consist of both positive and negative testing. Testing is primarily conducted using the CLI; however, several test steps have been included to utilize the web interface. The CLI and the Web interface modify the same underlying configuration file therefore duplication of all tests on both management interfaces would be highly redundant.

The Palo Alto Test Plan and Procedures document includes an introduction, test approach, and test environment. The test environment description includes the test network configuration, test coverage, test descriptions, test procedures/steps and expected results. Each test case is mapped to the appropriate security function and SFR and includes the Test Case identifier, Test case description/goal, Test design notes, Setup, Test Steps, Cleanup, Expected Results, Actual Results, Date Tested and Overall Pass/Fail status of the test.

The vendor test coverage rationale states that for each test case the expected behavior of the interface is tested and the test procedures (test prerequisites, test steps and expected results) adequately test the interface. Each of the SFRs claimed in the ST is tested at least once on each platform and all of the TSFIs defined in the FSP are tested at least once on each platform. Therefore, the test plan and procedures described provide adequate coverage for the TOE at EAL2. All tests passed.

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 three platforms: PA-4050, PA-2050, and PA-2020 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 three 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 suite across two of the claimed appliances, one from the low end group (PA-2050) and one from the high end group (PA-4050) both running PAN-OS version 2.1.7 and including the User Identification Agent v2.1.4 installed on a Windows PC. The chosen sample represented 50% of the vendor test suite and was determined based on the following factors:

- The test subset covers all of the TSFI (GUI, CLI, Network Interfaces, User Identification Agent, Firewall appliance to User Identification Agent)
- The test subset covers all security functions claimed in the ST with particular attention to the significant security function for this technology type, which is User Data Protection (Information Flow Control)
- The test subset covers Virtual Systems (found only on 4000 series) and the User Identification Agent

The following hardware was used to create the test configurations:

- PA-2050 and PA-4050 appliances running PAN-OS software version 2.1.7 and including the User Identification Agent client version 2.1.4
- User Identification Agent on a Windows machine
- Domain Controller
- Windows XP and Linux Server machines running Wireshark and WS_FTP software
- Management Switch
- 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 v2.1.7
- User Identification Agent v2.1.4
- Linux
- Windows
- Wireshark
- WS_FTP
- Active Directory
- Internet Explorer v.8
- Putty

The evaluation team performed the following additional functional tests:

- **Audit Review**. The evaluation team confirmed, through examination and analysis of the audit trail produced by running the vendor test sample and the evaluation team's own tests, that the ability to view the audit logs is appropriately restricted to the authorized administrators.
- **Auditable Events**. The evaluation team confirmed through examination and analysis of the audit trail produced by running the vendor test sample and the evaluation team's own tests, that all audit records specified in the ST can be generated by the TOE.
- **User Login**. The evaluation team confirmed via the GUI that users must be identified and authenticated before any further TSF-mediated action is allowed.
- **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 that can be one of the following:
  - Lock the account for a configured lockout period
  - Lock the account until a superuser unlocks it
- **Security Roles and Restrictions**. The evaluation team confirmed that each of the authorized administrator roles is appropriately restricted as described in the ST and the Admin guidance.
- **Configuration File Modification**. The evaluation team confirmed that the configuration file data cannot be directly accessed from the CLI and GUI management interfaces that do not provide the capability to traverse the directory structure of the underlying operating system. Furthermore, the team confirmed that any modifications made via the GUI and CLI appear in the same configuration files.
- **URL Filtering Profiles**. The evaluation team confirmed the TOE's ability to define a URL Filtering Profile including definition of a black list and a white list. The team verified that access to web sites listed on the black list will be blocked, while access to web sites on the white list will be allowed.
- **Consistent Time**. The evaluation team confirmed the consistency of timestamps documented in the audit log when user login is performed via the GUI.
- **Protection of Communications**. The evaluation team confirmed that the data transmitted between the firewall and the user identification agent is encrypted using one of the algorithms from the supported list of algorithms in the ST.

  Content Updates. The evaluation team confirmed the TOE's ability to perform dynamic updates via the GUI interface to install signature updates automatically downloaded from the Palo Alto Networks content server and to perform content updates manually via a downloaded file.

7.3. Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE and found one Cross-site scripting (XSS) vulnerability relevant to the TOE (CVE-2010-0475) that was fixed in the evaluated version of the TOE, version 2.1.7. The team verified the bug fix for this vulnerability during the onsite audit of the Palo Alto flaw remediation system. 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. The team also performed extensive penetration testing including two tests specifically related to the web server vulnerabilities found. In all cases, the tests passed as expected and the TOE was found to be secure.

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).
- **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.
- **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.
- **URL Encoding.** The evaluation team confirmed that the TOE's URL capture mechanism is not susceptible to URL encoding tricks.
- **Unsupported Options.** The evaluation team confirmed that the TOE will deny the session and remain stable when configured with unsupported cipher suites and SSL options.
- **Grep Command.** The evaluation team confirmed that the non-standard use of the grep command in the TOE does not make it vulnerable to an injection attack.
- **ICMP.** The evaluation team confirmed that when ping is enabled on the management interface, the TOE is not susceptible to well-known ICMP attacks.
- **SCP Command.** The evaluation team confirmed that the SCP command can be used to import a configuration and that the connection is encrypted.
- **Web Server.** The evaluation team confirmed that the TOE is not susceptible to a cross site scripting vulnerability and a URL Protocol Format String vulnerability related to the TOE's web server.

8. Evaluated Configuration

The evaluated version of the TOE is identified as the Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall, which includes the models PA-2020, PA-2050, PA-4020, PA-4050, and PA-4060 appliances running PAN-OS software version 2.1.7 and including the User Identification Agent client version 2.1.4.

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 2.1.7**. The firmware component that runs the appliance. 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 and a Command Line 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 version 2.1.4**. This is the client software program installed on one or more PCs on the protected network, it provides the firewall with the capability to automatically collect user-specific information that it uses in policies and reporting.

The physical boundary of the TOE comprises the firewall appliance (i.e., a PA-2020, PA-2050, PA-4020, PA-4050, or PA-4060 model appliance), together with the User Identification Agent component. The five models of the PA-2000 Series and PA-4000 Series Firewall differ in their performance capability, but they provide the same functionality, with the exception of virtual systems, which are only supported on the PA-4020, PA-4050, and PA-4060. The following table illustrates the differences, in terms of their external interfaces, between the various TOE models.

Table 2. Differences Between TOE Models

Interface	**PA-2020**	**PA-2050**	**PA-4020**	**PA-4050**	**PA-4060**
Ethernet ports (RJ-45 10/100/1000) for network traffic	12	16	16	16	—
SFP* ports for network traffic	2	4	8	8	4
XFP* ports for network traffic	—	—	—	—	4
Management port (RJ-45 to access device management port)	1	1	1	1	1
Console port (for connecting a serial console)	RJ-45	RJ-45	DB-9	DB-9	DB-9
High-availability (HA) ports (see Note 1)	—	—	2	2	2
USB port (see Note 2)	1	1	2	2	2
*SFP – Small Form-Factor Pluggable; XFP – 10 Gigabit Small Form-Factor Pluggable					
Note 1: The 4000 Series appliances provide 2 dedicated RJ-45 ports for high-availability control and synchronization. The 2000 Series appliances also support HA functionality, but do not have dedicated HA ports. Instead, two Ethernet network ports need to be used. Note 2: The USB ports are not functional (they are included for potential future use) and so are not covered by the evaluation.					

In the evaluated configuration, the TOE can be managed by a directly-connected console (i.e., connected to the Console port), which must be a VT-100 terminal or a device that can emulate a VT-100 terminal. The console is part of the operational environment and is expected to correctly display what is sent to it from the TOE. The TOE can also be managed by a computer directly connected to the Management port via an RJ-45 Ethernet cable (i.e., with no intervening network infrastructure). The Management port is an out-of-band management port that provides access to the GUI via HTTPS and to the CLI via SSH. The computer is part of the operational environment and required to have a web browser (for accessing the GUI) or SSH client (for accessing the CLI).

The TOE relies on third-party software and hardware components in the operating environment such as a Windows domain controller to be used with the User Identification Agent and management client PCs. 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, and Windows Server 2003 with SP2 or higher. The TOE also offers the capability to send logs as SNMP traps, Syslog messages, or email notifications and to use an NTP server to synchronize time. While these capabilities are not excluded from the TOE, they have not been evaluated and would rely on the use of SNMP, SMTP, Syslog and NTP servers being in the operating environment of the TOE.

Refer to Section 4.1 for further clarification of the scope of this evaluation.

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 “EAL2 augmented with ALC_FLR.2” certificate rating be issued for Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall.

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 3. TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures
ALC_FLR.2	Flaw reporting procedures
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – conformance
AVA_VAN.2	Vulnerability analysis

10. Validator Comments/Recommendations

1. The TOE does not support IPv6 policy enforcement. While the TOE provides very limited IPv6 support at the management interface, it does not secure IPv6 traffic or support IPv6 policy enforcement.
2. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.
3. The TOE is compliant with and meets all required functionality in the US Government Protection Profile for Traffic-Filter firewall in Basic Robustness Environments Version 1.1, July 25, 2007. It does not provide the following functions, which are not included in the PP:
    - FIA_SOS – The TOE does not provide a mechanism to enforce password complexity, however, Appendix D of the Palo Alto Network's Administrator Guide provides password complexity requirements for the evaluated configuration.
    - FTA_SSL – Session Locking and Termination – The TOE provides an idle timeout. Users can logout and log back in to resume where they left off, however, these activities may not be audited.
    - FTA_TAB – TOE Access Banners – The TOE does not provide advisory warnings prior to session establishment.
    - FTA_TAH -- TOE Access History – The TOE does not provide the successfully logged in user with information regarding previous attempts to establish a session automatically. This information can be actively viewed via the System Log.
4. The PP to which this TOE is compliant only requires a subset of the management functions claimed in FMT_MOF.1 to be audited. This subset consists of all functions listed in this requirement pertaining to audit. The TOE, however, audits all security management functions claimed in FMT_MOF.1 with only the following exceptions:
    - Viewing of user attributes
    - Viewing of information flow rules
    - Importing and Exporting of Configuration files
5. The TOE provides distinct views for traffic log, threat log, system log and configuration logs. There is no unified audit log view.
6. 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.
7. The use of Customized Administrator Roles has not been evaluated.
8. The TOE does not provide a warning when the audit logs reach full capacity, however, Appendix D of the Palo Alto Network's Administrator Guide provides guidance to the user of the evaluated configuration regarding setting up a process for clearing logs in order to keep the device functioning and to avoid overwriting logs before they are externally archived.
9. The TOE provides the ability to enable or disable the unzipping of files for threat scanning. Encrypted zip files will be bypassed by the threat scanning process; however, the TOE can be configured to deny encrypted zip files.
10. 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-2000 Series and PA-4000 Series Firewall Security Target,** Version 1.0, October 18, 2011.

13. Bibliography

- Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006, CCIMB-2006-09-001.
- Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-002.
- Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-003.
- Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004.
- Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall Security Target, Version 1.0, October 18, 2011.