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

Version 1.0
October 18, 2011

Prepared for:

Palo Alto Networks Inc.

3300 Olcott Street
Santa Clara, CA 95054

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive
Columbia, MD 21046

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE comprises the PA-2000 Series and Pa-4000 Series Firewall products from Palo Alto Networks. The PA-2000 Series Firewall consists of the PA-2020 and PA-2050 model appliances, while the PA-4000 Series Firewall consists of the PA-4020, PA-4050, and PA-4060 model appliances. The firewall appliances comprising the TOE are used to manage enterprise network traffic flows using function specific processing for networking, security, and management. These firewalls identify which applications are flowing across the network irrespective of port, protocol, or SSL encryption. The TOE supports Security Audit, Identification and Authentication, User Data Protection, Security Management and TSF Protection.

The Security Target contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE.
- Security Environment (Section 3)—specifies the assumptions and threats that define the security problem to be addressed by the TOE and its operational environment.
- Security Objectives (Section 4)—specifies the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions defining the security problem.
- IT Security Requirements (Section 5)—specifies a set of security functional requirements to be met by the TOE. The IT security requirements also provide a set of security assurance requirements that are to be satisfied by the TOE.
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the security functional requirements.
- Protection Profile Claims (Section 7)—provides rationale that the TOE conforms to the PP(s) for which conformance has been claimed.
- Rationale (Section 8)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall Security Target

ST Version – Version 1.0

ST Date – October 18, 2011

TOE Identification – Palo Alto Networks PA-2000 Series Firewall Models PA-2020 and PA-2050, and PA-4000 Series Firewall Models PA-4020, PA-4050 and PA-4060, with PAN-OS software version 2.1.7 and User Identification Agent client version 2.1.4

TOE Developer – Palo Alto Networks

Evaluation Sponsor – Palo Alto Networks

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

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

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, September 2007, Version 3.1, Revision 2, CCMB-2007-09-002
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, September 2007, Version 3.1, Revision 2; CCMB-2007-09-003
    - Part 3 Conformant
    - Assurance Level: EAL 2 augmented with ALC_FLR.2

1.3 Conventions, Terminology and Acronyms

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

Refer to the US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments, Version 1.1, for a complete list of terminology that may be used within this ST. In addition, the following terminology is used with specific meaning in this ST:

trusted/internal These terms refer to an organization's own networks that are to be protected by the TOE. The TOE documentation uses the term 'trusted zone' for those interfaces that connect only to the organization's internal networks. The PP uses the term 'internal' in its statements of threats, assumptions, objectives and SFRs to refer to the same concept. This ST uses the TOE's terminology ('trusted') in the TOE Description and TOE Summary Specification, but retains the PP's terminology ('internal') in those statements it reproduces from the PP.

untrusted/external These terms refer to networks, such as the Internet, that are external to an organization and from which the organization's own networks are to be protected by the TOE. The TOE documentation uses the term 'untrusted zone' for those interfaces that connect only to external networks. The PP uses the term 'external' in its statements of threats, assumptions, objectives and SFRs to refer to the same concept. This ST uses the TOE's terminology ('untrusted') in the TOE Description and TOE Summary Specification, but retains the PP's terminology ('external') in those statements it reproduces from the PP.

2. TOE Description

The Target of Evaluation (TOE) is Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall, which includes models PA-2020, PA-2050, PA-4020, PA-4050, and PA-4060. The firewalls included in the TOE provide policy-based application visibility and control to protect traffic flowing through the enterprise network. The TOE also includes the PAN-OS software version 2.1.7 and the User Identification Agent client version 2.1.4.

2.1 TOE Overview

The firewalls comprising the TOE are network firewall appliances used to manage enterprise network traffic flow using function specific processing for networking, security, and management. These firewalls let the administrator 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 TOE firewalls provide granular control over the traffic allowed to access the protected network. They allow an administrator to define security policies for specific applications, rather than rely on a single policy for connections to a given port number. For each identified application, the administrator can specify a security policy to block or allow traffic based on the source and destination zones, source and destination addresses, or application services.

The TOE provides the following security related features[1]:

- Application-based policy enforcement—the product uses a traffic classification technology named App-ID to classify traffic by application content irrespective of port or protocol. Protocol and port can be used in conjunction with application identification to control what ports an application is allowed to run on. High risk applications can be blocked, as well as high-risk behavior such as file-sharing. SSL encrypted traffic can be decrypted[2] and inspected.
- Threat prevention—the firewall includes threat prevention capabilities that can protect the network from viruses, worms, spyware, and other malicious traffic[3].
- Fail-safe operation—the firewall provides fault-tolerant operations where the firewall can be deployed in active/passive pairs so that if the active firewall fails for any reason, the passive firewall becomes active automatically with no loss of service.
- Management—each firewall can be managed through an intuitive GUI or a text-based command-line interface (CLI). Both interfaces provide an administrator with the ability to establish policy controls, provide the means to control what applications network users are allowed access to, and to control logging and reporting. These interfaces also provide dynamic visibility tools that enable views into the actual applications running on the network. The GUI can identify the applications with the most traffic and the highest security risks. The TOE offers the option to have all firewall devices managed centrally through the Panorama central management system. Note that Panorama is distributed under a separate license.

Deployment Types

The TOE can be deployed in the following modes:

- Virtual Wire Deployment—in a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together.

[1] Updated application definitions and threat signatures are available from a secure server operated by Palo Alto Networks. All connections to this server use SSL and provide for server authentication, message authentication and confidentiality. A signature check is performed on the software to ensure authenticity.

[2] Note that the cryptographic capabilities provided by the TOE have not been subject to FIPS 140 validation. The vendor asserts the correctness of the cryptographic capabilities.

[3] The ability of the TOE to block traffic based on detected threats has been evaluated, but the evaluation has not covered the completeness of the TOE's signature data or the efficacy of individual signatures.

- Layer 2 Deployment—in a Layer 2 deployment, the firewall provides switching between two or more networks. Each pair of interfaces must be assigned to a VLAN, and additional Layer 2 sub-interfaces can be defined as needed.
- Layer 3 Deployment—in a Layer 3 deployment, the firewall routes traffic between the two ports. An IP address must be assigned to each interface and a virtual router defined to route the traffic.
- Tap Mode Deployment—a network tap is a device that provides a way to access data flowing across a computer network. Tap mode deployment lets you passively monitor traffic flows across a network by way of a switch SPAN or mirror port. Since policy enforcement does not occur in a Tap Mode deployment, this mode of operation is not permitted for the TOE.

Firewall Policy Enforcement

The App-ID classification technology uses four classification techniques to determine exactly what applications are traversing the network irrespective of port number. As traffic flows through the TOE, App-ID identifies traffic using the following classification engines.

- Application Protocol/Port—App-ID identifies the protocol (such as TCP or UDP) and the port number of the traffic. Protocol/Port information is primarily used for policy enforcement, such as allowing or blocking a specific application over a specific protocol or port number, but is sometimes used in classification, such as ICMP traffic where the protocol is the primary classification method used.
- Application Protocol Decoding—App-ID's protocol decoders determine if the application is using a protocol as a normal application transport (such as HTTP for web browsing applications), or if it is only using the apparent protocol to hide the real application protocol (for example, Yahoo! Instant Messenger might hide inside HTTP).
- Application Signatures—App-ID uses context-based signatures, which look for unique application properties and related transaction characteristics to correctly identify the application regardless of the protocol and port being used.
- Heuristics—App-ID requires multi-packet heuristics for identifying some encrypted applications like Skype and encrypted Bittorrent. This component of App-ID identifies patterns across multiple packets to identify these more complex applications. The actual heuristics used are specific to an application and include checks based on such things as the packet length, session rate, and packet source. These heuristics are not configurable.

The application-centric nature of App-ID means that it can not only identify and control traditional applications such as HTTP, FTP, and SNMP, but it can also accurately identify many more applications based on application signatures and protocol decoders. These applications span across many categories defined to simplify the process of building security policy that matches an organization's information security policy.

Threat Prevention

The TOE includes a real-time threat prevention engine that inspects the traffic traversing the network for a wide range of threats. The threat prevention engine scans for all types of threats with a uniform signature format, and can identify and block a wide range of threats across a broad set of applications in a single pass. The threats that can be detected by the threat prevention engine include: viruses; spyware (inbound file scanning, and connections to infected web sites); application vulnerability exploits; and phishing URL blocking[4].

Management

The TOE provides a Web Management interface and a Command-Line interface. The Web interface provides a Graphic User Interface (GUI) for management and control of TOE configuration and monitoring over HTTP or HTTPS from an Internet Explorer (IE) or Firefox browser (access via HTTP is excluded from the evaluated configuration). The TOE supports IE version 5.5 and later, and Firefox 1.0 and later. The CLI provides text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port (access via Telnet is excluded from the evaluated configuration). The GUI can be accessed by a supported browser from a PC that is directly

[4] The ability of the TOE to block traffic based on detected threats has been evaluated, but the evaluation has not covered the completeness of the TOE's signature data or the efficacy of individual signatures.

connected to the firewall's Ethernet management port. The CLI can be accessed by a SSH client from a PC directly connected to the firewall's Ethernet management port, or by a direct serial connection to the firewall's console port using a VT-100 terminal or a device that can emulate a VT-100 terminal. The evaluated configuration does not cover access to the CLI or GUI through an intermediate network.

Fault Tolerance

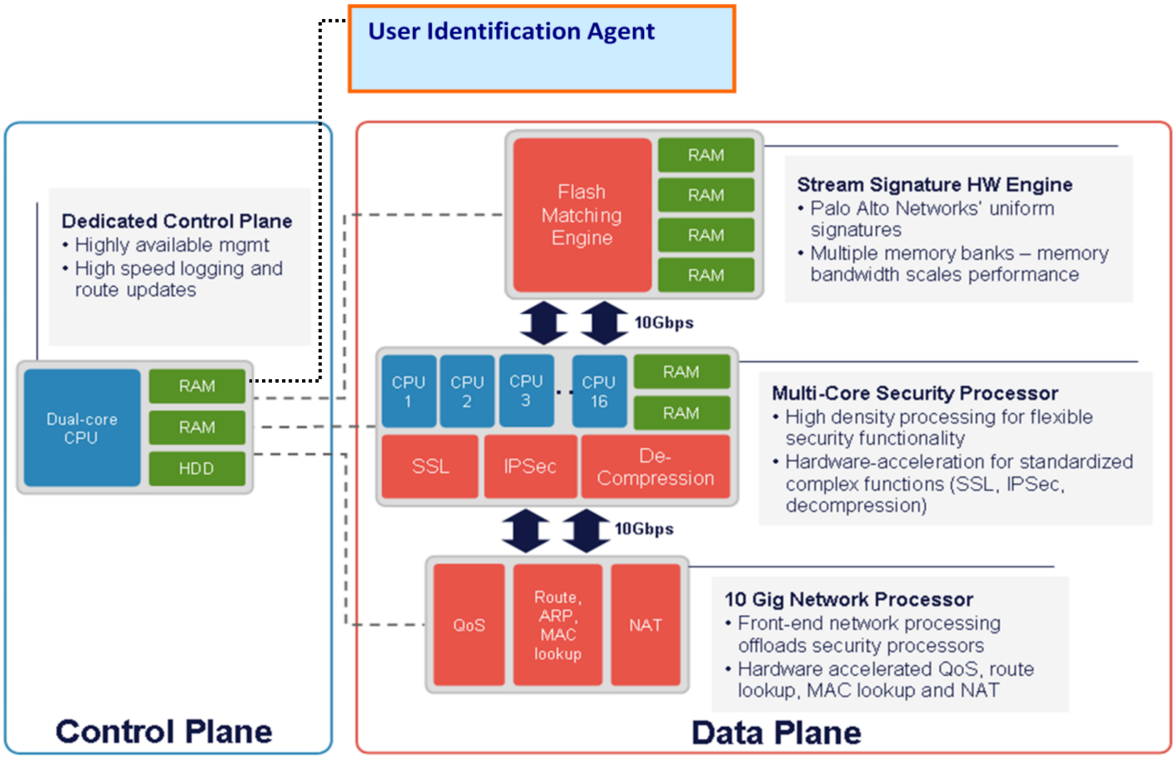
Fault-tolerant operation is provided when the TOE is deployed in active/passive pairs so that if the active firewall fails for any reason, the passive firewall becomes active automatically with no loss of service. A failover can also occur if selected Ethernet links fail or if one or more specified destinations cannot be reached by the active firewall.

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.

2.2 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. The User Identification Agent is installed on a separate PC[5] 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 make this information available to the firewall. 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 to include collected user information in policies and reports.

The following diagram depicts both the hardware and software architecture of the TOE.


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

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

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

Here is a summary of the functionality provided by each component of the system.

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.

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 in policies and reporting.

2.2.1 Physical Boundaries

The TOE consists of the following components:

- Hardware appliance—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 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 untrusted network to monitor network traffic so that the TSF can enforce the TSF security policy.
- User Identification Agent version 2.1.4—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 PA-2000 Series or PA-4000 Series 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 appliance models included in the TOE 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.

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. 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).

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.

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, and Windows Server 2003 with SP2 or higher.

2.2.2 Logical Boundaries

This section describes the logical scope of the TOE, i.e., the logical security features offered by the TOE, in terms of the following security functions: Security Audit, User Data Protection, Identification and Authentication, Security Management and TSF Protection. In addition, this section identifies any capability to be provided by the operational environment, and any TOE capabilities excluded from the scope of evaluation.

2.2.2.1 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.

2.2.2.2 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, file blocking profiles, and log forwarding profiles for traffic and threat logs (while system and config logs can be forwarded to external IT entities, this is not specified using log forwarding profiles)[6]. The profiles can identify which applications are inspected for viruses, a combination of methods to combat spyware, and the level of protection against known vulnerabilities. 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 used for SSL forward proxy to decrypt SSL traffic and apply policy rules before re-encrypting it to its destination. Note that the cryptographic mechanisms implemented in the TOE have not been subject to FIPS 140 validation. The correctness of their implementation is asserted by the vendor.

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.

[6] 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. This functionality is not security relevant and does not impair or affect the claimed security functionality in the TOE.

2.2.2.3 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.

2.2.2.4 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.

The product also supports a Custom Role Based Administration functionality that is excluded from the TOE.

2.2.2.5 TSF Protection

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.

2.2.2.6 Capabilities to be Provided by the Operational Environment

The TOE relies on the operational environment for the following components and capabilities:

- 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.
- 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.
- The User Identification Agent (UIA) relies on its underlying operating system for process separation and memory protection.
- The capability provided by the UIA relies on its being able to communicate with a Microsoft Windows domain controller in the operational environment.
- 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.

2.2.2.7 Product Capabilities Excluded from the Scope of Evaluation

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

- The TOE has the capability to support remote administration 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.

- 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.
- The deployment of the TOE in Tap Mode is excluded from the evaluated configuration.
- The use of a RADIUS server and Captive Portal are not supported in the evaluated configuration.
- The TOE 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 PA-2000 Series and PA-4000 Series firewall products to be managed from a centralized management server, allowing a single management console for managing multiple devices.
- 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.
- The use of Telnet to connect from the TOE to another IT entity is excluded from the evaluated configuration.
- 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.
- The ability to download and install an update of the TOE software from the management interface is excluded from the evaluated configuration.
- The TOE 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.
- 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.

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

- 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.
- 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.
- The use of an external NTP server is allowed in the evaluated configuration, but has not been subject to evaluation.
- 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.
- 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.
- The TOE’s ability for administrators to create definitions for applications that are not recognized by the TOE has not been subject to evaluation.
- 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.

2.3 TOE Documentation

Palo Alto Networks offers a series of documents that describe the installation of the Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall products, as well as guidance for subsequent use and administration of the applicable security features. These documents include:

- Palo Alto Networks Administrator’s Guide, Release 2.1.7, including Appendix D, which provides specific information regarding the Common Criteria configuration
- Pan OS Command Line Interface Reference Guide, Release 2.1.

3. Security Environment

The TOE is intended for a basic robustness environment. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. In general, basic robustness results in “good commercial practices” that counter threats based on casual and accidental disclosure or compromise of data protected by the TOE.

This section describes the assumptions and threats that are relevant to both the TOE and its environment. The first section describes the secure usage assumptions, which are those items that the TOE itself cannot implement or enforce. The next two sections cover the threats that are expected to exist in a basic robustness environment and are grouped into threats to be addressed by the TOE and threats to be addressed by the TOE environment. Both the assumptions and the threats are reproduced from the US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007, except as described in Section 7 of this ST.

3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

A.UIA_ONLY The PC used for the UIA component is dedicated to this function and is not used for any other purpose.

A.PHYSEC The TOE is physically secure.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.GENPUR There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT 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.

A.NOREMO All human users including the authorized administrators can not access the TOE remotely from the internal or external networks.

A.NOREMACC Authorized administrators may not access the TOE remotely from the internal and external networks.

A.CONSOLE 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.

3.2 Threats Addressed by the TOE

The following threats are addressed by the TOE.

T.NOAUTH 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.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.REPLAY An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.

T.ASPOOF An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

T.MEDIAT An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

T.OLDINF 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.

T.AUDACC 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.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

T.AUDFUL 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 attackers actions.

3.3 Threats Addressed by the TOE Environment

The threat possibility discussed below must be countered by procedural measures and/or administrative methods.

T.TUSAGE The TOE may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons.

4. Security Objectives

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats, comply with defined organizational security policies, and address applicable assumptions.

The security objectives are reproduced from the US Government Protection Profile for Traffic-Filter firewall in Basic Robustness Environments Version 1.1, July 25, 2007.

4.1 Security Objectives for the TOE

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

O.MEDIAT The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

4.2 Security Objectives for the Operating Environment

The security objectives for the operating environment are reproduced from the US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environment, Version 1.1, July 25, 2007, except as described in Section 7 of this ST. All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

OE.UIA_ONLY The PC used for the UIA component is dedicated to this function and is not used for any other purpose.

OE.PHYSEC The TOE is physically secure.

OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

OE.PUBLIC The TOE does not host public data.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

OE.DIRECT 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.

OE.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

OE.NOREMACC Authorized administrators may not access the TOE remotely from the internal and external networks.

OE.CONSOLE 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.

OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

5. IT Security Requirements

This section specifies the security requirements for the TOE. The statement of security functional requirements reproduces the security functional requirements (SFRs) specified in the US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environment, Version 1.1, July 25, 2007 with operations completed as appropriate. The ST also includes several security functional requirements that are not claimed in the PP. The requirements are all drawn from the CC Part 2.

The Security Assurance Requirements (SARs) are those requirements comprising Evaluation Assurance Level 2 (EAL2) as defined in the CC Part 3.

5.1 TOE Security Functional Requirements

The following table identifies the security functional requirements that are satisfied by the TOE.

Table 5-1 Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_SAR.3: Selectable audit review
	FAU_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
FCS: Cryptographic support	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.1: Subset residual information protection
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of Authentication
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.2: Secure security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_SMR.1: Security roles
FPT: Protection of the TOE security functions	FPT_FLS.1: Failure with preservation of secure state
	FPT_ITT.1: Basic internal TSF data transfer
	FPT_STM.1: Reliable time stamps
FRU: Resource utilisation	FRU_FLT.1: Degraded fault tolerance

5.1.1 Security Audit

5.1.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All relevant auditable events for the ***minimal or basic level*** of audit specified in Table 5-2 and

c) [**the event in Table 5-2 listed at the "extended" level**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject**s** identit**ies**, outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**information specified in column four of Table 5-2**].

Table 5-2 Auditable Events

Functional Component	**Level**	**Auditable Event**	**Additional Audit Record Contents**
FMT_SMR.1	minimal	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FIA_UID.2	basic	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	extended	Use of the **following** functions listed in this requirement ~~pertaining to audit.~~**:** • **start-up and shutdown** • **create, delete, and modify information flow security policy rules that permit or deny information flows** • **create, delete, and modify user attribute values defined in FIA_ATD.1** • **modify and set the threshold for the number of permitted authentication attempt failures** • **modify and set the time and date** • **archive, create, delete, empty, and review the audit trail** • **install application definition and threat signature updates.**	The identity of the authorized administrator performing the operation.

5.1.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**an authorized administrator**] with the capability to read [**all audit trail data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.4 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches and sorting***] of audit data based on:

[**a)** **presumed subject address;**
b) **ranges of dates;**
c) **ranges of times;**
d) **ranges of addresses**].

5.1.1.5 Protected Audit Trail Storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent]*** modifications to the audit records**.**

5.1.1.6 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***prevent auditable events, except those taken by the authorized administrator***] and [**shall limit the number of audit records lost**] if the audit trail is full.

5.1.2 Cryptographic Operation

5.1.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**pseudo random number generator**] and specified cryptographic key sizes [**128bits and 256 bits**] that meet the following: [**X9.31**].

5.1.2.2 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwrite**] that meets the following: [**FIPS 140-2 level 1**].

5.1.2.3 Cryptographic Operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform [**SSL encryption and decryption of SSL encrypted traffic received by the TOE; and encryption and decryption of communications between the agent and the firewall**] in accordance with a specified cryptographic algorithm: [**AES-CBC, 3DES-EDE-CBC, and RC4**] and cryptographic key sizes [**that are at least 128 binary digits in length**] that meet the following: [**FIPS 197, FIPS PUB 463, and none (for RC4)**].

5.1.3 Information Flow Control

5.1.3.1 Subset Information Flow Control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] on:

a) [**subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;**
b) **information: traffic sent through the TOE from one subject to another;**
c) **operation: pass information**].

5.1.3.2 Simple Security Attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] based on **at least** the following types of subject and information security attributes:

[**a) subject security attributes:**

- **presumed address;**
- **and no other subject security attributes**

b) information security attributes:

- **presumed address of source subject;**
- **presumed address of destination subject;**
- **transport layer protocol;**
- **TOE interface on which traffic arrives and departs;**
- **Service;**
- **User;**
- **Port;**
- **Source and destination security zones;**
- **Traffic payload].**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

[**a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;**
- **the presumed address of the source subject, in the information, translates to an internal network address;**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network.**

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;**
- **the presumed address of the source subject, in the information, translates to an external network address;**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network.**]

FDP_IFF.1.3 The TSF shall enforce the [**following additional security profiles, when configured in an information flow security policy that matches the information security attributes:**

- **Antivirus profile—the TSF will inspect an application for viruses against the TSF's antivirus signatures and take action (e.g., generate alert, deny or drop application traffic) when a virus is detected.**
- **Antispyware profile—the TSF will apply a specified mechanism (download protection, website blocking, traffic detection) to counter detected spyware.**
- **Vulnerability protection profile—the TSF will apply a specified mechanism (generate an alert, drop application traffic, block all packets, reset the session) when the TSF detects a vulnerability.**
- **URL filtering profile—the TSF will block access to specific web sites, or generate an alert when a specified web site is accessed.**
- **File blocking profile—the TSF will block selected file types, or generate an alert when a specified file type is detected**].

FDP_IFF.1.4 The TSF shall provide the following [**none**].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

[**a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;**

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

]

Application Note: The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses. A "service", listed in FDP_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number.

5.1.3.3 Subset Residual Information Protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] the following objects: [**resources that are used by the subjects of the TOE to communicate through the TOE to other subjects**].

Application Note: If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out an interface, these bits would be considered a "resource". The intent of the requirement is that these bits shall not contain the remains of information that had previously passed through the TOE. The requirement is met by overwriting or clearing resources, (e.g. packets) before making them available for use.

5.1.4 Identification and Authentication

5.1.4.1 Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [1..10]***] unsuccessful authentication attempts occur related to [**user login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**based on administrator configuration, lock the user account for a configured period of time, or lock the user account until it is unlocked by an administrator**].

5.1.4.2 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:
[**a) identity;**
b) association of a human user with the authorized administrator role;
c) authentication Data
d) the virtual system(s) that a user can access].

5.1.4.3 Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**identification as stated in FIA_UID.2**] on behalf of the authorized administrator accessing the TOE to be performed before the authorized administrator is authenticated.

FIA_UAU.1.2 The TSF shall require each authorized administrator to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator.

5.1.4.4 User Identification Before Any Action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security Management

5.1.5.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***perform***] the functions: [

a) start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

~~**d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);**~~

e) modify and set the threshold for the number of permitted authentication attempt failures ~~(if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)~~;

f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures ~~(if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)~~;

~~**g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);**~~

h) modify and set the time and date;

i) archive, create, delete, empty, and review the audit trail;

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup;

~~**l) additionally, if the TSF supports remote administration from either an internal or external network:**~~

- ~~**enable and disable remote administration from internal and external networks;**~~
- ~~**restrict addresses from which remote administration can be performed;**~~

m) [install application definition and threat signature updates]]

to [**an authorized administrator**].

5.1.5.2 Secure Security Attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [**cryptographic keys**].attributes

5.1.5.3 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] to provide [***restrictive***] default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the role [**authorized administrator (this role includes the superuser, superuser (read only) -- – referred to as superreader in the CLI, device admin, device admin (read only) -- – referred to as devicereader in the CLI, Vsys admin, and Vsys admin (read only) -- – referred to as vsysreader in the CLI)**].

FMT_SMR.1.2 The TSF shall be able to associate **human** users with the authorized administrator role.

5.1.6 Protection of the TSF

5.1.6.1 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.7 Fault Tolerance

5.1.7.1 Degraded Fault Tolerance (FRU_FLT.1)

FRU_FLT.1.1 The TSF shall ensure the operation of [**policy enforcement**] when the following failures occur [**when a selected Ethernet links fail, or if one or more specified destinations cannot be reached by the active firewall**].

5.1.8 Protection of the TSF

5.1.8.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**when the active firewall fails because a selected Ethernet links fails, or when one or more specified destinations cannot be reached by the active firewall**].

5.1.8.2 Basic Internal TSF Data Transfer (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure and modification***] when it is transmitted between separate parts of the TOE.

5.2 TOE Security Assurance Requirements

The TOE assurance requirements are EAL2 augmented by ALC_FLR.2 as shown in the table below. All assurance requirements are summarized in the table below.

Table 5-3 Assurance Requirements: EAL2 Augmented

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative user guidance
ALC: Life-cycle support	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: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

5.2.1 Class ADV: Development

5.2.1.1 ADV_ARC.1 Security Architecture Description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 ADV_FSP.2 Security-enforcing Functional Specification

ADV_FSP.2.1D The developer shall provide a functional specification

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 ADV_TDS.1 Basic Design

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1-5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TSF.1.6C The mapping shall demonstrate that all behavior described in the TOE is mapped to the TSFIs that invoke it.

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Class AGD: Guidance Documents

5.2.2.1 AGD_OPE.1 Operational User Guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to user the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall describe, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 AGD_PRE.1 Preparative Procedures

AGD_PRE.1.1D The developer shall provide the Toe including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.1E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Class ALC: Life-Cycle Support

5.2.3.1 ALC_CMC.2 Use of a CM System

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 ALC_CMS.2 Parts of the TOE CM Coverage

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 ALC_DEL.1 Delivery Procedures

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.4 ALC_FLR.2 Flaw Reporting Procedures

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users' reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the Toe.

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Class ATE: Test

5.2.4.1 ATE_COV.1 Evidence of Coverage

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 ATE_FUN.1 Functional Testing

ATE_FUN.1.1D The developer shall test the TSF and document the result.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results, and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed an describe the scenarios for performing each tests. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.3 ATE_IND.2 Independent Testing – Sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test as subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Class AVA: Vulnerability Assessment

5.2.5.1 AVA_VAN.2 Vulnerability Analysis

AVA_VAN.2.1D The developer shall provide the TOE for testing.

AVA_VAN.2.1C The TOE shall be suitable for testing.

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the TOE security functions and how they address the security functional requirements..

6.1 TOE Security Functions

The following security functions are defined for the TOE:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TSF Protection.

6.1.1 Security Audit

The TOE is capable of generating audit records for a number of security events and provides the appropriate level of audit details (minimal, basic, or extended) depending on the audited events. Each audit record includes, in addition to the specific details listed below, at least the date and time of the event, type of event, subject identities, outcome (success or failure) of the event. The auditable events are as follow:

- Modification to the group of users that are part of the authorized administrator role. Audit records include the identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
- All use of the identification mechanism. Audit records include the user identities provided to the TOE.
- All use of the authentication mechanism. Audit records include the user identities provided to the TOE.
- All decisions on request for information flow control. Audit records include the presumed addresses of the source and destination subject.
- Changes to the time. Audit records details include the identity of the authorized administrator performing the operation.
- Use of the management functions including:
  - Start-up and shutdown of the TOE
  - Creation, deletion, and modification of information flow security policy rules that permit or deny information flows
  - Creation, deletion, and modification of user attribute values
  - Setting and modification of the threshold for the number of permitted authentication attempt failures
  - Setting and modification of the time and date
  - Archive, creation, deletion, emptying, and review of the audit trail
  - Installation of application definition and threat signature updates.

  The content of the audit records includes the identity of the authorized administrator performing the operation.
- The startup and shutdown of the audit function is audited and performed in conjunction with the startup and shutdown of the system itself.

The audit trail comprises four separate logs:

- Configuration log—include events such as when an administrator configures the security policies, or when an administrator configures which events are audited.
- System log—records user login and logout.
- Traffic log—records the traffic flow events.
- Threat log—records the detection and prevention by the TOE of any threats.

Through the CLI and the GUI the TOE provides the ability to review the audit trail and to search and sort the audit records based on presumed subject address, ranges of addresses; ranges of date; and range of time. In accordance with PD-0159, the TOE implements the sorting of audit data as follows:

- The audit data is automatically pre-sorted by timestamp.
- The ability to search the audit data by IP address can be performed via multiple queries for a single IP address or by a single query for multiple IP addresses. Multiple IP addresses can be defined as discrete IP addresses or as a range of IP addresses.
    - For example, a query via the GUI would appear as follows: "(addr.src in 10.16.0.60) or (addr.src in 10.16.0.50)".
    - Searching can also be done on a set of IP addresses using subnet notation as in: "(addr.src in 10.16.0.0/24)" which would cover all addresses from 10.16.0.0-10.16.0.0.255.
    - Compound expressions that pair the previous two examples with a date range are also supported as in: "(addr.dst in 10.0.0.255/24) and (receive_time geq '2010/03/01 00:00:00') and (receive_time leq '2010/03/19 00:00:00')"

The TOE stores the audit records locally and protects them from unauthorized deletion by allowing only the authorized administrator to access the audit trail. The TOE does not provide an interface where a user can modify the audit records, thus it prevents unauthorized modification to the audit records. The audit trail delete/empty function can only be performed via the CLI using the "clear" command. This function cannot be performed via the GUI.

If the traffic or threat logs become full, the TSF will stop accepting traffic, log the audit trail full event to the system log and will stop performing all auditable events except those undertaken by an authorized administrator. When either the traffic or threat log becomes full, the Control Plane immediately communicates with the Data Plane to prevent new connections from being created until the audit trail is restored, thereby limiting the loss of audit records. The number of audit records lost when the system is under minimal stress is zero.

It should be noted that the TOE does not stop receiving traffic if either the configuration log or the system log fills up. Instead, the TOE overwrites the oldest records in these logs. Since these logs record only auditable actions taken by the administrator, this behavior is consistent with the specification of FAU_STG.4. The Administrator's Guide provides guidance to users on how to regularly export audit logs so as to avoid data loss.

The TOE provides administrators with the ability to manually archive and backup the audit trail before clearing it. The GUI provides a means to backup a selected log file as a file of comma-separated values (CSV format), while the CLI provides the `scp` command that can be used to securely copy files (including specified log files) to another IT entity.

The Security Audit security function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE provides the ability to audit the required auditable events and record within each audit event the required date/time, event type, subject, and event outcome.
- FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 — the GUI provides authorized administrator the capability to review the audit records including the options to search and sort the audit records.
- FAU_STG.1, FAU_STG.4 — The TOE stores all audit logs locally and protects the audit records from unauthorized deletion by ensuring that only authorized administrators can access them. The TSF prevents

audit data loss, by preventing all auditable events except those undertaken by authorized administrators in order to limit the number of audit records that are lost when the audit trail is full.

- FPT_STM.1 — The TOE provides reliable time stamps for the logs.

6.1.2 Identification and Authentication

The TSF maintains user accounts which it uses to control access to the firewall. When an administrator creates a new user account, the administrator specifies a user name (i.e. user identity), a password, and a role. The TOE stores a one-way hash of the user password, rather than the password itself. Only one role is specified for each user account. The TSF uses the user name and password attributes to identify and authenticate a user when that user performs a login via the GUI or the CLI. The TOE uses the role attribute to determine user permissions and control the actions that the user can perform using the GUI or the CLI. The superuser role has permissions to manage user accounts and to create new user accounts. The TOE identifies and authenticates all users accessing the TOE via the GUI and the CLI. It should be noted the TOE does not enforce any restrictions on password choice (such as minimum length or complexity). However, Appendix D of the Palo Alto Networks Administrator's Guide provides the following advice to the administrator regarding password selection: passwords should be at least 8 characters; passwords should employ combinations of numeric and upper and lower case alphabetic characters; passwords should not be easily guessable (e.g., birth dates or names of family members).

The TSF provides a mechanism to lock out user accounts when an excessive number (defined by an administrator, in the range 1 to 10) of consecutive unsuccessful login attempts have been made. The TSF can be configured to unlock affected accounts after a configurable period of time (one minute or more), or to maintain the account lockout until an administrator unlocks the account.

Interfaces and security zones can be grouped into virtual systems, and then managed independently of each other. For example, the administrator can define virtual systems for the interfaces associated with specific departments or customers, and can then customize the administrative access, security policies, and logging for each department or customer. The administrator can also define administrator accounts that provide administrative or view-only access to a single virtual system. Initially all interfaces, zones, and policies belong to the default virtual system (vsys1).When multiple virtual systems are enabled, the TSF also maintains a list of the virtual systems that a user can access. Note that administrator accounts can be defined that are limited to the administration of a specific virtual system(s).

The Identification and Authentication security function is designed to satisfy the following security functional requirements:

- FIA_AFL.1—the TSF is able to lock a user's account when a configurable number of consecutive failed authentication attempts have occurred, and keep the account locked for a configurable period of time, or until the account is unlocked by an administrator.
- FIA_ATD.1 — the TSF maintains user accounts which contain the attributes user identity, password, role and the virtual systems that can be accessed. It uses these attributes to identify and authenticate users, and to determine a user's access permissions.
- FIA_UID.2, FIA_UAU.1 — the TSF identifies and authenticates all users accessing its functions and data.

6.1.3 User Data Protection

The TOE enforces an unauthenticated information flow control SFP to control the type of information that is allowed to pass through the TOE. The enforcement process involves the TOE applying policies and profiles rules to determine what actions to take. Policies are applied from most specific to least specific and if no policy applies, the packet is dropped. Incoming traffic is compared against the rules defined in the following categories of administrator configured policies: security policies, Network Address Translation (NAT) policies and SSL decryption policies.

- Security policies specify whether to block or allow a new network session based on the traffic attributes, such as the application, source and destination security zones, the source and destination addresses and the application service (such as HTTP). Security policies can also specify security profiles and they can be restricted to selected users or applications. Each security policy can specify one or more security profiles of types:

  - Antivirus profiles —identify which applications are inspected for viruses and the action taken when a virus is detected (i.e. alert or deny/drop the application traffic).
  - Antispyware profiles —determine the combination of methods used to combat spyware — download protection, web site blocking, and detection of traffic from installed spyware.
  - Vulnerability protection profiles —determine the level of protection against attempts to exploits system vulnerabilities including all known critical, high and medium-severity threats. The possible actions taken when vulnerabilities are detected include options to generate an alert, drop the application traffic, keep all packets from continuing, and reset (the client, the server, or both).
  - URL filtering profiles — block access to specific web sites and web site categories, or generate an alert when the specified web sites are accessed. These profiles can also define a "black list" of web sites that are always blocked (or generate alerts) and a "white list" of web sites that are always allowed.
  - File blocking profiles — blocks selected file types from being uploaded and/or downloaded, or generate an alert when the specified file types are detected.
  - Log forwarding profiles – determines whether in addition to the local logging performed by default, traffic and threat log entries are sent as SNMP traps, Syslog messages, or email notifications. Note that traffic logs record information about each traffic flow, and threat logs record the threats or problems with the network traffic such as virus or spyware detection. (As noted previously, this functionality is not security relevant and has not been subject to evaluation).
  - Security Profile Groups — which combines antivirus, anti-spyware, vulnerability, and file blocking profiles assigned together.

- NAT policies specify whether source or destination IP addresses and ports are converted between public and private addresses and ports. For example, private source addresses can be translated to public addresses on traffic sent from a trusted zone to an untrusted zone. NAT policy rules are based on the source and destination zones, the source and destination addresses, and the application service. The NAT policy rules are compared against the incoming traffic in sequence, the first rule that match the incoming traffic is applied.
- Secure Socket Layer (SSL) decryption policies specify the SSL traffic to be decrypted so that security policy rules can be applied. SSL decryption policy rules specify the categories of URLs traffic to decrypt or not decrypt. SSL decryption is enabled using a policy rulebase so that traffic can be selectively decrypted (or allowed to pass through) based on source/destination IP, source user, and source/destination zone. If the SSL session requires mutual authentication, decryption will not succeed. The SSL policy rules are also applied in sequence to the incoming traffic.

Ethernet ports on the firewall can be configured as Layer 2, Layer3 and virtual wire interface types. A zone identifies one or more interfaces on the firewall and interfaces are grouped according to the relative risk of the traffic they carry. Separate zones must be created for each type of interface and each interface must be assigned to a zone before it can process traffic. Security policies can be defined only between zones of the same types. To define each security policy rule, the source and destination zones of the traffic must be specified.

The TOE provides the capability to define security policies that are restricted to specific applications or users. The TOE identifies several categories of applications including: business-system applications (i.e. auth-service, databases, office program, and software updates); collaboration applications (i.e. email, instant messaging, voip-video, social networking, and web posting); general internet applications (i.e. file sharing and internet utility); media applications (i.e. audio streaming, gaming and photo video); networking applications (i.e. encrypted-tunnel, ip-protocol, proxy, remote-access, and routing); and unknown applications. When defining security policies that are restricted to a specific application, the authorized administrator can select one or more services to limit the port numbers the applications can use. The default service is any, which allows all TCP and UDP ports. The HTTP and HTTPS services are predefined but additional service definitions can be added, and services that are often assigned together can be combined into service groups to simplify the creation of security policies.

The User Identification Agent (UIA) component contributes to the enforcement of the unauthenticated information flow SFP by providing mappings of IP addresses to user names. The UIA retrieves the user ID from the Active Directory domain controller in the operational environment and forwards it to the firewall, which uses it to identify the user. The user identity is used in policies and reporting, as described below.

When the TOE receives a packet it first determines if it represents a new connection or if it is part of an existing session. If it is part of an existing session, the traffic is processed based on the parameters of the existing session (see below for additional details). If it is a new connection, the TOE retrieves the source and destination zones and performs an initial policy lookup. When performing a security policy lookup for a new session, the TOE will attempt to map the source IP address to a specific username based on the user to IP mapping information received from the UIA. If a username cannot be determined, the security policy lookup will only match rules with “any” specified in the user column. If a policy is defined for the zone pair (i.e., source and destination zones), a session is created and the packet proceeds. By default, traffic between each pair of security zones is blocked until at least one rule is added to allow traffic between the two zones. Sessions are not created for a new connection if there is no policy defined for the zone pair; or if there is an initial deny rule for the application service (i.e., service-HTTP, service-https) matching the traffic with no applications defined.

The TOE performs the following steps when processing traffic:

- The traffic is passed through the Application Identification and Application Decoders to determine what type of application is creating the session[7]. It is in this step that the URL is captured and categorized for use later.
- Once the application is known the TOE performs a policy lookup with the following information:
    - The source/destination IP address
    - The source/destination security zone
    - The application and service (port and protocol)
- Traffic is dropped and a session is not created in the following circumstances:
    - the source address of the incoming traffic corresponds to the IP address of an untrusted broadcast network or loopback network
    - the incoming traffic is received from the untrusted network but has a source address that corresponds to the trusted network
    - traffic is received from the trusted network but has a source address that corresponds to the untrusted network.
- If a policy is not found, or if it is found and the policy specifies a deny action then the packet is dropped and the session is deleted.
- If a security policy is found the policy rules are compared against the incoming traffic in sequence, the first rule that matches the traffic is applied. If the traffic does not match any of the rules, the traffic is blocked. If a NAT policy or an SSL policy is found, the policy rules are also compared against the incoming traffic in sequence.
- If the application flow is allowed and no further security profiles are applied then it is forwarded. If the session had previously been SSL that had been decrypted it will be encrypted before transmission.
- If the application is allowed and there are additional security profiles set it will be sent to the stream engine processor.
- When traffic is sent to the TOE, the unified stream based signatures are applied to the flow. Based on the security profiles defined for the session and depending on what is discovered in the flow the system can allow, deny without log or deny with log.

[7] 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.

The TSF allocates and releases the memory resources used for network packet objects. Both when it receives data from the network and when it transmits data to the network, it ensures that the buffers are not padded out with previously transmitted or otherwise residual information.

The TOE implements SSLv3 and is able to decrypt SSL encrypted traffic received by the TOE in order to apply the security policy rules; it re-encrypts the traffic before passing it to its destination. The TOE uses a random number generator for key generation. Cryptographic keys are generated on the dataplane and destroyed when the session is destroyed. SSLv3 is also used in the TOE to protect the integrity of communication between the User Identification Agent and the firewall.

The supported cipher suites are:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_AES_256_CBC_SHA

The User Data Protection security function is designed to satisfy the following security functional requirement:

- FDP_IFC.1, FDP_IFF.1 — The TSF controls the flow of information through the TOE ensuring that only traffic allowed by configured policies are permitted.
- FDP_RIP.1 — The TOE ensures that any previous information content of buffers used for network packets is not available when a new buffer is either received by the TOE from the network interface or transmitted by the TOE.
- FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FMT_MSA.2 — The TSF performs encryption and decryption of network packet according to configured policy. It ensures that the key values used for encryption are secure. When the TOE receives encrypted traffic, it decrypts it and applies the information flow rules and re-encrypt it before sending it to its destination.

6.1.4 Security Management

The TSF provides a GUI management interface and a text-based CLI to support security management of the TOE. Both the GUI and the CLI are accessed via direct connection to the box. The management interfaces enable the authorized administrator to configure the TOE functions and to manipulate TOE data. The management interfaces provide the following capabilities:

- Start-up and shutdown the TOE.
- Manage the settings for identification and authentication, including:
  - Creating, deleting, modifying and viewing user security attributes, including the capability for users to change their own passwords.
  - Setting the values that control the user account lockout mechanism. Specifically, the administrator can specify the number of consecutive failed authentication attempts (between 1 and 10) after which the user account is locked (a value of 0 disables the account lockout mechanism), and the number of minutes (1 to 60) for which the account remains locked (a value of 0 locks the account until it is unlocked by a Superuser).
  - Unlocking a locked user account.
- Modify and set the time and date.
- Backup and restore the TOE configuration using SCP to securely export and import files to and from an external IT entity.
- Install updates to application definitions and threat signatures. Updates can be performed on-line (i.e., the TOE connects directly to the Palo Alto secure support portal to download the updates) or off-line (i.e., updates are downloaded to a separate computer and then uploaded to the TOE via the GUI).

Through the management interfaces, authorized administrators configure policies to set which external IT entities can communicate with the TOE; policies that contain the information flow security rules including the type of traffic allowed through the TOE, the ports and protocol that can be used; and the type of applications allowed to send information through the TOE. The policies also describe the encryption/decryption rules, to determine if traffic received by the TOE should be decrypted, analyzed and re-encrypted before it is sent to the destination address or if it should pass through without being decrypted.

In addition, the management interfaces are used to manage the audit function and review the audit trail. Audit management includes the ability to archive and backup the audit trail.

The TOE implements the following roles with the corresponding privilege levels:

Table 6-1 Administrative Roles

Roles	Privilege Level
Superuser	Has full access to the firewall and can define new administrator accounts.
Superuser (Read Only) – referred to as superreader in the CLI	Read-only access to the current device
Device Admin	Full access to a selected device, except for defining new accounts and virtual systems, modifying the system time, importing configuration files, and creating local configuration backups on the firewall.
Device Admin (Read Only) – referred to as devicereader in the CLI	Read-only access to the selected device
Vsys Admin	Full access to a selected virtual system on a specific device (if multiple virtual systems are enabled). Vsys admins cannot perform device tasks such as creating user accounts, modifying the system time, or deleting device-wide logs. Vsys admins can access logs specific to their virtual system only from the web interface. Vsys admins can export configuration for backup purposes using the **scp export** CLI command.
Vsys Admin (Read Only) – referred to as vsysreader in the CLI	Read-only access to a selected virtual system on a specific device (if multiple virtual systems are enabled)

The Superuser and Device Admin Roles are considered authorized administrators. Both can manage the audit function and manage the information flow attributes. The main difference is that the Device Admin cannot create new user accounts. Read only administrators are able to view/read audit records, but cannot delete audit records or make configuration changes.

One user account is pre-defined in a newly installed TOE. The role associated with this pre-defined admin account is superuser.

The Security Management security function is designed to satisfy the following security functional requirements:

- FMT_SMR.1 — The TSF defines the authorized administrator role and associates users with that role.
- FMT_MSA.3 — The TSF restricts to the authorized administrator the ability to specify alternative initial values to override default restrictive values of the security attributes within the scope of the UNAUTHENTICATED SFP.
- FMT_MOF.1 — the management interfaces provide the ability to manage the security functions provided by the TOE.

6.1.5 TSF Protection

Fault-tolerant operation is provided when the TOE is deployed in active/passive pairs. If the active firewall fails because a selected Ethernet links fails or if one or more specific 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 protect the integrity of communication between the User Identification Agent and the firewall. The firewall invokes the cryptographic functions when it initiates communication with the Agent to collect user information. The TOE uses a random number generator for key generation. Cryptographic keys are generated on the dataplane and destroyed when the session is destroyed.

The TSF Protection security function is designed to satisfy the following security functional requirements:

- FRU_FLT.1 and FPT_FLS.1 — The TSF ensures that the information flow control are applied even when the primary firewall is unavailable.
- FPT_ITT.1 — The TSF ensures the protection of communication between the user identification agent and the firewall.

7. Protection Profile Claims

As documented in this Security Target (ST), the TOE (Palo Alto Networks PA-2000 Series and PA-4000 Series Firewall) complies with the US Government Protection Profile for Traffic filter Firewall in Basic Robustness Environment, Version 1.1, July 25, 2007.

The Security Environment, Objectives, and Requirements in this ST have been reproduced from the Traffic Filter Firewall PP, as indicated below:

No new threats have been introduced and all threats have been included except for the following:

- The ST removes the threat T.PROCOM; it does not apply because the ST explicitly disallows the use of remote administration in the evaluated configuration.
- The ST removes the threats T.REPEAT and T.REPLAY because these threats are present when human users connect remotely to the TOE user interfaces. The PP maps these threats to O.SINUSE and the ST removes this security objective.

All assumptions have been included except for the following:

- The ST removes A.REMACC because the ST explicitly disallows remote administration. The ST adds the assumption A.NOREMACC to address the exclusion of remote administration.
- The ST adds the assumption A.CONSOLE to address the need to have a direct console connection to the management console port, since remote access to the management console is not permitted in the TOE.
- The ST adds the assumption A.UIA_ONLY to address the need to have the PC used as a platform for the UIA component of the TOE dedicated to the UIA application.

All the Traffic Filter Firewall PP security objectives have been included with the following modifications:

- The ST removes the security objectives O.ENCRYP and O.SINUSE because they address requirements for the use of encryption when an authorized administrator performs administrative functions on the TOE remotely and any users attempt to authenticate at the TOE from the connected network. The ST disallows remote access to the user/administrator interfaces in the TOE.

The ST adds the following security objectives for the operational environment to address the assumptions added by the ST: OE.UIA_ONLY; OE.NOREMACC; and OE.CONSOLE. In addition, the ST labels all security objectives for the operational environment with 'OE.' Instead of 'A.' as used in the PP. This is consistent with the practice of the vast majority of ST documents.

All operations on the requirements have been completed in compliance with the PP, as indicated using bold and bold-italic text in Section 5.1.

The following requirement is omitted from the ST.

- FIA_UAU.4 is not being claimed in the ST. Remote Administration is explicitly disallowed in the evaluated configuration. The PP allows an ST to exclude FIA_UAU.4 if the product does not have Remote Administration capability, but if the capability is claimed the cryptographic mechanisms used to secure the Remote Administration traffic must be FIPS Certified. The TOE offers the capability for remote administration, but this communication is not protected by a FIPS certified mechanism. Because of this, the ST explicitly disallowed the use of remote administration in the evaluated configuration, which voids this requirement.

The following requirements are added to the ST.

- FAU_SAR.2 is added to the ST to address the TOE capability to protect the audit records and to restrict access to the audit trail.
- FCS_CKM.1 and FCS_CKM.4 are added to the ST to address encryption and decryption of encrypted traffic received by the TOE.
- FMT_MSA.2 is added to the ST to address the dependency of the FCS_CKM requirement components.

- FRU_FLT.1 and FPT_FLS.1 are added to the ST to address the fault tolerant capability provided by the TOE.
- FPT_ITT.1 is added to the ST to address protection of communication between the separate components of the TOE.

The following additional tailoring of specific security requirements has been performed:

- FIA_AFL.1: The ST replaces the version of this SFR specified in the PP with the standard version specified in CC Part 2, since the PP rendering relates specifically to external IT entities, which are unable to authenticate to the TOE. The TOE satisfies this SFR for administrators logging on at the console.
- FIA_ATD.1.1: The ST specifies “authentication data” as the “other user security attributes” to be determined by the ST author.
- FDP_IFF.1.1 b): The ST specifies “user”, “port” and “source and destination security zones” as the “other information security attributes to be determined by the ST author”.
- FDP_IFF.1.3: The ST replaces the “none” specified by the PP with requirements for the TSF to apply specified security profiles, when configured, to traffic that matches a configured security policy.
- FMT_MOF.1.1: The following changes are made:
    - The ST removes “d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);”.
    - The ST modifies e) to remove “(if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)”.
    - The ST modifies f) to remove “(if the TOE supports authorized IT entities and/or remote administrations from either an internal or external network)”.
    - The ST removes “g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external entities);”.
    - The ST removes “l) additionally, if the TSF supports remote administration from either an internal or external network: enable and disable remote administration from internal and external networks; restrict addresses from which remote administration can be performed;”.
    - The ST completes the assignment operation in m) by specifying additional management capabilities.
- FCS_COP.1: The ST replaces the version of this SFR specified in the PP with a statement of the capabilities provided by the TOE. The PP includes FCS_COP.1 to provide encryption of remote administrative sessions, but the ST explicitly disallows remote administration, so FCS_COP.1 as specified in the PP does not apply to this TOE. Instead, the ST specifies FCS_COP.1 to require data encryption and decryption of encrypted traffic received by the TOE.
- FAU_GEN.1: The ST modifies the statement of FAU_GEN.1 to specify all the auditable management capabilities from FMT_MOF.1.

The removal of the audit event associated with FIA_AFL.1 from the FAU_GEN.1 requirement is valid because the auditable event from the PP is related to authentication failure by external IT entities, which are not permitted in the evaluated configuration for this TOE. The FIA_AFL.1 requirement in this ST pertains to authentication of administrators.

The removal of the audit event associated with FCS_COP.1 from the FAU_GEN.1 requirement is valid because the auditable event from the PP is related to cryptographic operations associated with remote administrations, which is not permitted in the evaluated configuration for this TOE. The FCS_COP.1 requirement in this Security Target pertains to the communication between TOE components.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Strength of Functions
- Requirement Dependencies
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

The US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environment (Traffic-filter Firewall PP) provides rationale for the security objectives demonstrating that security objectives are suitable to cover the intended environment. The rationale (provided in Section 6.1 and Section 6.2 of the Traffic-filter Firewall PP) is valid for the PP objectives reproduced in this ST with the following additions:

The ST replaces A.REMACC (from the PP) with OE.NOREMACC because the ST explicitly disallows remote administration of the TOE. OE.NOREMACC ensures that authorized administrators do not access the TOE remotely either from the internal or the external network.

A.CONSOLE is included in the ST as an assumption, and OE.CONSOLE is included as the corresponding security objective, to address the need for the environment to provide a VT-100 terminal for direct console access to the management console.

A.UIA_ONLY is included in the ST as an assumption, and OE.UIA_ONLY is included as the corresponding security objective, to indicate clearly that the UIA is on a dedicated computer.

8.2 Security Requirements Rationale

Section 6.3 the US Government Traffic Filter Firewall PP provide rationale for the security requirements, demonstrating that the security requirements are suitable to address the IT security objectives. This rationale is valid for the PP requirements reproduced in the ST and is not further discussed.

The ST includes security functional requirements that are additional to those of the PP. The dependencies of these requirements are all satisfied.

FRU_FLT.1 and FPT_FLS.1 ensures that the TOE continues to perform information flow control in case of failure. These components trace back to and aid in meeting the O.SECSTA security objective.

FCS_CKM.1, FCS_CKM.4, FCS_COP.1 and FMT_MSA.1 were added in support of the FDP_IFC.1 to allow the TSF to enforce the SFP on encrypted traffic. These components trace back to and aid in meeting the O.MEDIAT security objective.

FPT_ITT.1 ensures that communication between separate TOE components is protected. This component traces back to and aid in meeting the O.SELPRO security objective.

FIA_AFL.1 ensures the TOE can be protected from repeated attempts by an attacker to guess an administrator’s password. This requirement traces back to and aids in meeting O.SELPRO.

Table 8-1 Mapping of SFRs to Security Objectives

	O.MEDIAT	O.AUDREC	O.SECSTA	O.SELPRO
FAU_SAR.2		X		
FCS_CKM.1	X			
FCS_CKM.4	X			
FIA_AFL.1				X
FMT_MSA.1	X			
FRU_FLT.1			X	
FPT_FLS.1			X	
FCS_COP.1	X			
FPT_ITT.1				X

8.3 Security Assurance Requirements Rationale

The US Government Protection Profile for Traffic-Filter Firewall in Basic Robustness Environment provides rationale for the security assurance requirements, demonstrating that they are sufficient given the statement of security environment and security objectives. The rationale is provided in Section 6.4 of the US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environment and is valid for this ST as no new security requirements or security objectives were added.

While the ST adds several security functional requirements to those of the PP, the PP rationale for the security assurance requirements still apply. Basic robustness is still chosen for the TOE because the threats of malicious attacks identified in the ST are still no more than moderate.

8.4 Requirement Dependency Rationale

The US Government Traffic Filter Firewall PP requirements have been evaluated and it has been determined that all dependencies have been satisfactorily addressed in the US Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environment. The following table therefore analyzes the dependencies only of the requirements that have been added to this ST.

Table 8-2 Functional Requirements Dependencies

Requirement	Dependencies	Included
FAU_SAR.2	FAU_SAR.1	Yes
FCS_CKM.1	FCS_CKM.2 orFCS_COP.1 FCS_CKM.4, FMT_MSA.2	Yes — FCS_COP.1 FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Yes — FCS_CKM.1, FMT_MSA.1
FIA_AFL.1	FIA_UAU.1	Yes

Requirement	Dependencies	Included
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	Yes — FDP_IFC.1, FMT_SMR.1. The PP has rationale for exclusion of FMT_MSA.1
FRU_FLT.1	FPT_FLS.1	Yes
FPT_FLS.1	None	

8.5 Extended Components Rationale

There are no extended requirements in this Security Target.

8.6 PP Claims Rationale

See Section 7, Protection Profile Claims.