Palo Alto Networks PA-200, PA-500, PA-7050, PA-2000 Series, PA-3000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 6.0.3

Security Target

Version 3.1
February 5, 2015

Prepared for:
Palo Alto Networks Inc.

4401 Great America Parkway
Santa Clara, CA 95054

Prepared By:
Leidos (formerly SAIC)

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive
Columbia, MD 21046

Revision History

Version	Date	Description	Author
0.3	31 August 2010	Initial version	SAIC
0.4	14 May 2011	Added PA-5000 platforms	Wes Higaki
0.5	29 December 2011	Changed product name and updated ST according to ETR	N. Campagna
0.6	17 January 2012	Updating ST according to ETR	N. Campagna
0.7	1 February 2012	Further ETR updates	N. Campagna
0.8	28 February 2012	EAL 4 Augmentation list and further ETR updates	Jake Bajic
0.9	10 April 2012	X9.31 RNG update and further ETR updates	Jake Bajic
0.10	25 May 2012	ETR updates	Jake Bajic
0.11	14 August 2012	ETR updates	Jake Bajic
0.12	11 September 2012	ETR updates	Jake Bajic
0.13	13 November 2012	ETR updates	Jake Bajic
0.14	29 November 2012	Accepted changes and removed comments, added algorithm certification numbers.	Jake Bajic
0.15	8 February 2013	Test VOR updates	Jake Bajic
0.16	25 February 2013	Pre Final VOR updates	Jake Bajic
0.17	1 March 2013	Minor updates	Jake Bajic
0.18	5 April 2013	Final VOR updates	Jake Bajic
1.0	10 April	Minor updates after Final VOR presentation	Jake Bajic
2.0	25 February 2014	Assurance Continuity Updates	Jake Bajic
3.0	5 September 2014	Assurance Continuity Updates	Jake Bajic
3.1	5 February 2015	Assurance Continuity Updates – updated FIPS certificate number	Jake Bajic

Table of Contents

1. SECURITY TARGET INTRODUCTION 5

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 5
1.2 CONFORMANCE CLAIMS 6
1.3 CONVENTIONS, TERMINOLOGY AND ABBREVIATIONS 6

2. TOE DESCRIPTION 8

2.1 TOE OVERVIEW 8
2.2 TOE ARCHITECTURE 10
2.2.1 Physical Boundaries 12
2.2.2 Logical Boundaries 14
2.2.3 Product Capabilities not supported in the TOE 16
2.3 TOE DOCUMENTATION 19

3. SECURITY PROBLEM DEFINITION 20

3.1 ASSUMPTIONS 20
3.2 THREATS 20
3.3 ORGANIZATIONAL SECURITY POLICIES 21

4. SECURITY OBJECTIVES 23

4.1 SECURITY OBJECTIVES FOR THE TOE 23
4.2 SECURITY OBJECTIVES FOR THE OPERATING ENVIRONMENT 24

5. IT SECURITY REQUIREMENTS 25

5.1 EXTENDED COMPONENT DEFINITIONS 25
5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 25
5.2.1 Security Audit 28
5.2.2 Cryptographic Support 37
5.2.3 User Data Protection 39
5.2.4 Identification and Authentication 42
5.2.5 Security Management 43
5.2.6 Protection of the TSF 46
5.2.7 Resource Allocation 47
5.2.8 TOE Access 48
5.2.9 Trusted Path/Channels 48
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 49
5.3.1 Development (ADV) 50
5.3.2 Guidance Documents (AGD) 52
5.3.3 Life-cycle Support (ALC) 53
5.3.4 Tests (ATE) 55
5.3.5 Vulnerability Assessment (AVA) 57

6. TOE SUMMARY SPECIFICATION 58

6.1 TOE SECURITY FUNCTIONS 58
6.1.1 Security Audit 58
6.1.2 Cryptographic Support 63
6.1.3 Identification and Authentication 64
6.1.4 User Data Protection 65
6.1.5 Security Management 72
6.1.6 TSF Protection 74
6.1.7 Resource Utilization 76
6.1.8 TOE Access 76
6.1.9 Trusted Path/Channels 77

7. PROTECTION PROFILE CLAIMS 78

8. RATIONALE 80

8.1 SECURITY OBJECTIVES RATIONALE 80
8.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 80
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 81
8.4 REQUIREMENT DEPENDENCY RATIONALE 81
8.5 PP CLAIMS RATIONALE 81

LIST OF TABLES

Table 1: TOE Security Functional Requirements 28
Table 2: Audit Events 35
Table 3: Assurance Components 49
Table 4: Requirement Dependency Summary 81

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 is the next-generation firewall running PAN-OS v6.0.3, with User Identification Agent, v6.0.2-3, provided by Palo Alto Networks Inc. The next-generation firewall includes the PA-200, PA-500, PA-7050, PA-2020, PA-2050, PA-3020, PA-3050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060 appliances, which are used to manage enterprise network traffic flows using function specific processing for networking, security, and management. The next-generation firewalls identify which applications are flowing across the network, irrespective of port, protocol, or SSL encryption. The User Identification Agent (installed on a PC in the network) communicates with the domain controller to retrieve user-specific information. It allows the next-generation firewall to automatically collect user information and include it in policies and reporting.

The 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 Problem Definition (Section 3)—describes the assumptions, threats, and organizational security policies that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the objectives necessary to counter the defined threats and satisfy the assumptions and organizational security policies
- IT Security Requirements (Section 5)—provides 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-200, PA-500, PA-7050, PA-2000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 6.0.3 Security Target

ST Version – See ST title page

ST Date – See ST title page

TOE Identification – Palo Alto Networks next-generation firewall models PA-200, PA-500, PA-7050, PA-2020, PA-2050, PA-3020, PA-3050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060 with PAN-OS v6.0.3 and the User Identification Agent v6.0.2-3

TOE Developer – Palo Alto Networks Inc.

Evaluation Sponsor – Palo Alto Networks Inc.

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:

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 Extended

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

This ST and the TOE it describes meet all of the Security Functional Requirements (SFRs) of the following Protection Profile (PP):

- U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, July 25, 2007.

This ST and the TOE it describes are conformant to the following assurance package:

- EAL4 augmented with ALC_FLR.2, and ATE_DPT.3

1.3 Conventions, Terminology and Abbreviations

1.3.1 Conventions

Where requirements are drawn from the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, the requirements are copied from the Protection Profile and all operation conventions employed by the Protection Profile are removed, with the exception of the iteration convention. Otherwise, only operations performed in this Security Target are identified.

Where requirements are drawn from the Common Criteria (and are not found in the Protection Profile), the requirements are copied and the operations performed in this Security Target are identified.

Where applicable, the following conventions are used to identify operations:

- **Iteration:** Iterated requirements (components and elements) are identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).
- **Assignment:** Assignments are identified in brackets and bold (e.g., **[assigned value]**).
- **Selection:** Selections are identified in brackets, bold, and italics (e.g., **[*selected value*]**).
    - Assignments within selections are identified using the previous conventions, except that the assigned value would also be italicized and extra brackets would occur (e.g., **[*selected value [assigned value]*]**).
- **Refinement:** Refinements are identified using bold text (e.g., **added text**) for additions and strike-through text (e.g., ~~deleted text~~) for deletions.

1.3.2 Terminology and Abbreviations

The following terms and abbreviations are used in this ST:

Security policy	Provides the firewall rule sets that specify whether to block or allow network connections.
Security profile	A security profile specifies protection rules to apply when processing network traffic. The profiles supported by the TOE include Antivirus, Anti-spyware, Vulnerability Protection, File Blocking, and Data Filtering. Security profiles are specified in security policies.

Security zone	A grouping of TOE interfaces. Each TOE interface must be assigned to a zone before it can process traffic.
SFP	Security Function Policy—set of rules describing specific security behavior enforced by the TOE security functions and expressible as a set of security functional requirements.
SSL	Secure Sockets Layer—a cryptographic protocol that provides security for communications over networks.
Virtual system	Virtual systems allow the TOE administrator to customize administration, networking, and security policies for network traffic belonging to specific user groupings (such as departments or customers).
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

In addition, refer to the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, for a list of terminology that may be used within this ST.

2. TOE Description

The Target of Evaluation (TOE) is Palo Alto Networks next-generation firewall, which includes models PA-200, PA-500, PA-7050, PA-2020, PA-2050, PA-3020, PA-3050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060, each equipped with PAN-OS v6.0.3, and the User Identification Agent, v6.0.2-3. The next-generation firewall is a firewall that provides policy-based application visibility and control to protect traffic flowing through the enterprise network.

2.1 TOE Overview

The next-generation firewalls are network firewall appliances used to manage enterprise network traffic flow using function specific processing for networking, security, and management. The next-generation firewalls let the administrator specify security policies based on an accurate identification of each application seeking access to the protected network. The next-generation firewall uses packet inspection and a library of applications to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports. The next-generation firewall also supports the establishment of Virtual Private Network (VPN) connections to other next-generation firewalls or third party security devices.

A next-generation firewall is typically installed between an edge router or other device facing the Internet and a switch or router connecting to the internal network. The Ethernet interfaces on the firewall can be configured to support various networking environments, including: Layer 2 switching and VLAN environments; Layer 3 routing environments; transparent in-line deployments; and combinations of the three.

The next-generation 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 next-generation firewall products provide the following security related features:

- 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 and inspected.
- Threat prevention — the firewall includes threat prevention capabilities that can protect the network from viruses, worms, spyware, and other malicious traffic.
- Traffic visibility — the firewall includes the capability to generate extensive reports, logs, and notification mechanisms that provide detailed visibility into network application traffic and security events.
- Fail-safe operation — the firewall can be configured for 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 a Graphical User Interface (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. When configured in a Common Criteria mode of operation, the GUI is secured using HTTP over TLSv1.0. When used in Common Criteria compliant deployments, the CLI may be used for maintenance, recovery and debugging purposes, which is outside the normal operation of 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 application-centric nature of App-ID means that it cannot only identify and control traditional applications such as SMTP, FTP, and SNMP, but it can also accurately identify many more applications through the use of protocol decoders and application signatures. These applications are categorized in order to simplify the process of building a security policy that matches an organization's information security policy.

Threat Prevention

The next-generation firewall 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/malicious URLs.

App-ID and Threat Prevention Signature Updates

App-ID and threat prevention signatures (collectively known as content updates) may be updated periodically using the dynamic updates feature of the firewall. The TOE can be instructed to contact Palo Alto Networks' update server to download new content updates as they are made available. The connection to the update server is secured with TLS v1.0 and is secured using FIPS-approved algorithms. For an additional layer of protection, Palo Alto Networks has chosen to sign (using RSA-2048) and encrypt (using AES-256) all content that is downloaded to the firewall.

Management

The next-generation firewall provides a Web Management interface and a Command-Line interface. The Web interface provides a GUI for management and control of TOE configuration and monitoring over HTTP or HTTPS from an Internet Explorer (IE, version 7 or later), Firefox (version 3.6 or later), Safari (version 5 or later), and Chrome (version 11 or later) browser. The CLI provides text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port. In Common Criteria mode, the firewall must be administered via HTTPS. HTTP-based management is excluded from the evaluated configuration. The CLI may be used for maintenance, recovery and debugging purposes, which is outside the normal operation of the TOE.

Note that some additional management features are not permitted in the evaluated configuration (see section "Product Capabilities not supported in the TOE" for a detailed list of excluded features).

User Identification Agent

User Identification Agent (UIA) version 6.0.2-3 – client software program installed on one or more PCs on the protected network. The UIA provides the firewall with the capability to automatically collect user-specific information that is used in security policy enforcement and reporting. The UIA is not related to Identification and Authentication.

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.

Common Criteria Compliant Mode of Operation

The TOE is compliant with the capabilities outlined in this Security Target only when operated in Common Criteria mode. Common Criteria mode is a special operational mode in which the FIPS 140-2 requirements for startup and conditional self-tests as well as algorithm selection are enforced. In this mode, only FIPS-approved and FIPS-allowed cryptographic algorithms are available. The TOE will also enable certain PP-related functionality when configured in this mode of operation. The PP-related functions include selective audit, expired private key zeroization, and scheduled or on-demand cryptographic and software integrity self-tests.

2.2 TOE Architecture

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

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

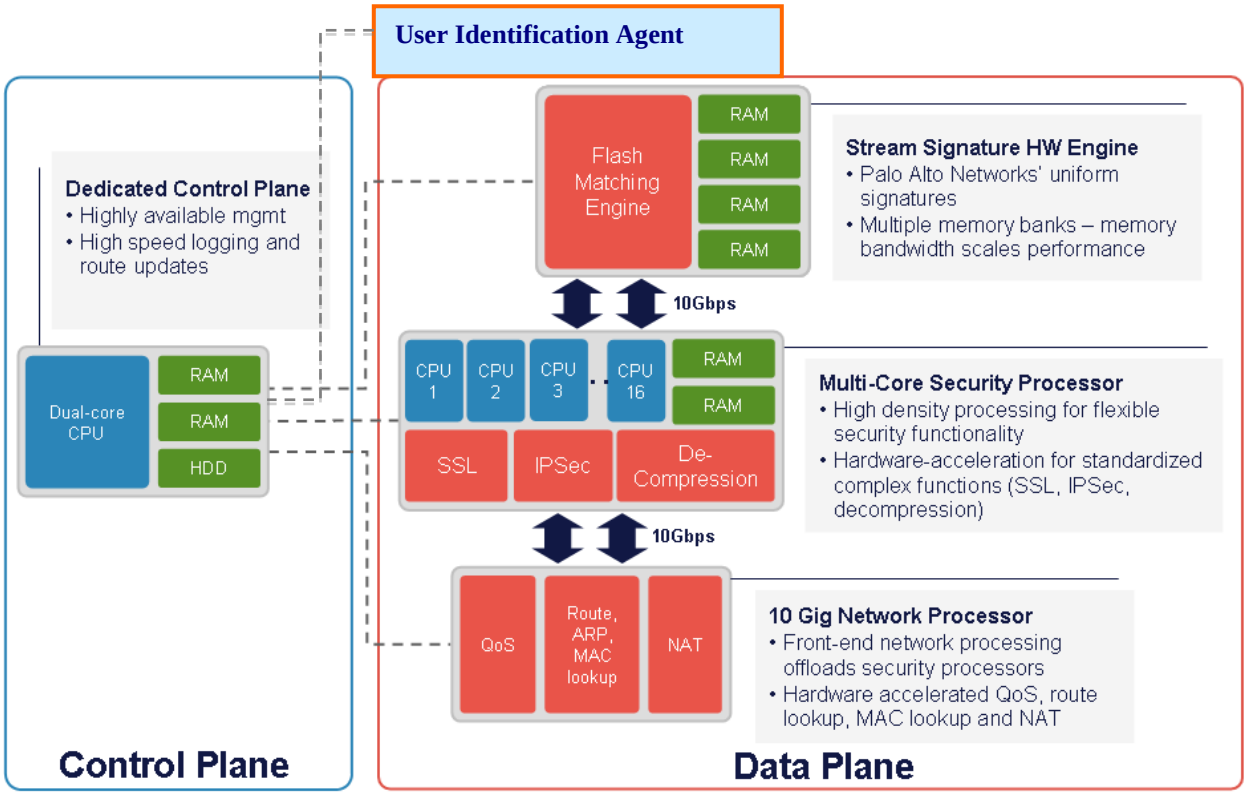

Figure 1: TOE Architecture

The control plane includes a dual core CPU, with dedicated memory and a hard drive for local log, configuration, and software storage. The data plane includes three components—the network processor, the security processor, and the stream signature processor—each with its own dedicated memory and hardware processing.

In summary, the functionality provided by each component of the system is as follows:

Control Plane

The control plane provides all device management functionality, including:

- All management interfaces: CLI (direct console access— used for maintenance, recovery and debugging purposes, which is outside the normal operation of the TOE), GUI interface, syslog logging, SNMP, and ICMP
- Configuration management of the device, such as controlling the changes made to the device configuration, as well as the compilation and pushing to the dataplane of a configuration change
- Logging infrastructure for traffic, threat, alarm, configuration, and system logs
- Reporting infrastructure for reports, monitoring tools, and graphical visibility tools (reporting is excluded from the evaluated configuration)
- Administration controls, including administrator authentication and audit trail information for administrators logging in, logging out, and configuration changes.
- Interactions with the UIA to retrieve the user to IP address mapping information that is used for policy enforcement.

Data Plane

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

- All networking connectivity, packet forwarding, switching, routing, and network address translation
- Application identification, using the content of the applications, not just port or protocol
- SSL forward proxy, including decryption and re-encryption
- Policy lookups to determine what security policy to enforce and what actions to take, including scanning for threats, logging, and packet marking
- Application decoding, threat scanning for all types of threats and threat prevention
- Logging, with all logs sent to the control plane for processing and storage

The TOE's SSL decryption feature uses an SSL proxy to establish itself as a man-in-the-middle proxy, which decrypts and controls the traffic within the SSL tunnel that traverses the TOE. The SSL proxy acts as a forward proxy (internal client to an external server). The certificates used by the TOE during forward proxying include as much relevant data from the external server's original certificate as possible (i.e., validity dates, certificate purpose, common name, and subject information). For inbound connections (external client to internal server), the TOE can decrypt incoming traffic and control the traffic within the SSL tunnel. SSL decryption is configured as a rulebase in which match criteria include zone, IP address, and User-ID. SSL proxy is configured by creating a Certificate Authority certificate (CA cert) on the firewall. When a client attempts to connect with a remote server, if a decryption policy is matched, the firewall will create a connection with the server and another connection with the client, inserting itself in the middle. The firewall will copy the subject information, validity information, and common name into a new certificate that is signed by the CA cert. If the firewall trusts the issuer of the server's certificate, it will sign the newly generated server cert with a trusted CA cert. If the firewall does not trust the issuer of the server's certificate, it will sign the newly generated server cert with an untrusted CA cert, thereby relaying the untrusted nature of the certificate to the client. A new public/private key pair is generated for each new SSL server to which the client's connect.

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

User Identification Agent

The user identification agent is a client software program installed on one or more PCs on the protected network to obtain user-specific information. The agent can be installed on any PC running Windows XP with SP2 (or higher than SP2), or Windows Vista, or Windows Server 2003 32bit with SP2 (or higher than SP2), or Windows Server 2008 32bit and 64bit. The agent communicates with a Microsoft Windows Domain Controller to obtain user information (such as user groups, users, and machines deployed in the domain) and makes the information available to the firewall, which uses it for policy enforcement and reporting. The UIA maintains mapping information received from the Domain Controller, which it synchronizes to the firewall table. The UIA only works with IPv4 addresses and does not work with IPv6 addresses.

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 6.0.3 – the firmware component that runs the appliance. PAN-OS is built on top of a Linux kernel and runs along with Appweb (the web server that Palo Alto Networks uses), crond, syslogd, and various vendor-developed applications that implement PAN-OS capabilities. PAN-OS provides the logical interfaces for network traffic. PAN-OS runs on both the Control Plane and the Data Plane and provides all firewall functionalities provided by the TOE, including the threat prevention capabilities as well as the identification and authentication of users and the management functions. PAN-OS provides unique functionality on the two planes based on the applications that are executing. The Control Plane provides a GUI Web management interface to access and manage the TOE functions and data. The Data Plane provides the external interface between the TOE and the external network to monitor network traffic so that the TSF can enforce the TSF security policy.
- User Identification Agent (UIA) version 6.0.2-3 – client software program installed on one or more PCs on the protected network. The UIA provides the firewall with the capability to automatically collect user-specific information that is used in security policy enforcement and reporting.

The physical boundary of the TOE comprises the firewall appliance (PA-200, PA-500, PA-7050, PA-2020, PA-2050, PA-3020, PA-3050, PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, and PA-5060), together with the User Identification Agent (UIA) component. The nine models of the next-generation firewall differ in their performance capability, but they provide the same security functionality, with the exception of virtual systems, which are supported by default (without an additional license) on the PA-4020, PA-4050, PA-4060, PA-5020, PA-5050, PA-5060, and PA-7050. The PA-2000 Series can support virtual systems with the purchase of an additional license. The PA-500 cannot support virtual systems. Virtual systems specify a collection of physical and logical firewall interfaces that should be isolated. Each virtual system contains its own security policy and its own set of logs that will be kept separate from all other virtual systems.

The firewall appliance attaches to a physical network and includes the following ports:

- PA-200: 8 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)
- PA-500: 8 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)
- PA-2020: 12 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 2 Small Form-Factor Pluggable (SFP) Gbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)

- PA-2050: 16 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 4 Small Form-Factor Pluggable (SFP) Gbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); and 1 RJ-45 port for connecting a serial console (management console port)
- PA-3020/PA-3050: 12 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 8 Small Form-Factor Pluggable (SFP) Gbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); 1 RJ-45 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization
- PA-4020/4050: 16 RJ-45 10/100/1000 ports for network traffic (Ethernet ports); 8 Small Form-Factor Pluggable (GFP) Mbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); 1 DB-9 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization
- PA-4060: 4 XFP 10 Gbps ports for management traffic; 4 Small Form-Factor Pluggable (SFP) Mbps ports for network traffic, 1 RJ-45 port to access the device CLI or GUI through an Ethernet interface (management ports); 1 DB-9 port for connecting a serial console (management console port); and 2 RJ-45 ports for high-availability (HA) control and synchronization
- PA-5020: 12 RJ-45 10/100/1000 ports for network traffic. 8 Small Form-Factor Pluggable (SFP) ports for network traffic. One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two RJ-45 ports for high-availability (HA) control and synchronization.
- PA-5050: 12 RJ-45 10/100/1000 ports for network traffic. Eight Small Form-Factor Pluggable (SFP) ports for network traffic. Four SFP+ ports for network traffic. One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two RJ-45 ports for high-availability (HA) control and synchronization.
- PA-5060: 12 RJ-45 10/100/1000 ports for network traffic. Eight Small Form-Factor Pluggable (SFP) ports for network traffic. Four SFP+ ports for network traffic. One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two RJ-45 ports for high-availability (HA) control and synchronization.
- PA-7050: 12 gig copper ports for network traffic, eight Small Form-Factor Pluggable (SFP) ports for network traffic and four SFP+ ports for network traffic per blade (6 blades max). One RJ-45 port to access the device management interfaces through an Ethernet interface. One RJ-45 port for connecting a serial console. Two QSFP ports for high-availability (HA) control and synchronization.

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

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

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

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

The port for connecting a serial console (DB-9 in PA-4000 series and RJ-45 for PA-500, PA-7050, PA-2000, PA-3000, and PA-5000 series) is not part of the TOE evaluated configuration, as it is enabled only for output in Common Criteria mode.

2.2.2 Logical Boundaries

The logical boundaries of the TOE are described in terms of the security functions provided by the next-generation firewall. These comprise: Security Audit; Cryptographic Support; User Data Protection; Identification and Authentication; Security Management; TSF Protection; Resource Utilization; TOE Access; and Trusted Path/Channels. The CMVP has validated the cryptographic module and issued the following certificate:

Certificate No. 2323 - PA-200, PA-500, PA-2000 Series, PA-3000, PA-4000 Series, PA-5000, and PA-7050 Series Firewalls by Palo Alto Networks. Please reference the NIST website, Validation Lists for Cryptographic Standards at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2323

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). The management GUI is used to review the audit trail. The management GUI offers options to sort and search the audit records, and to include or exclude auditable events from the set of audited events. The TOE stores the audit trail locally. The TOE protects the audit trail by providing only restricted access to it; by not providing interfaces to modify the audit records. The TOE also provides a time-stamp for the audit records.

In addition, the TOE monitors various events occurring on the firewall (such as authentication failures and information flow policy failures) and will generate an alarm if the number of such events reaches a configured limit, indicating a potential security violation.

2.2.2.2 Cryptographic Support

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

2.2.2.3 User Data Protection

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

In addition, each security policy can also specify one or more security profiles, including: antivirus profiles; antispyware profiles; vulnerability protection profiles; and file blocking profiles. The profiles can identify which applications are inspected for viruses, a combination of methods to combat spyware, the level of protection against known vulnerabilities, and which type of files can be uploaded or downloaded. The TOE compares the policy rules against the incoming traffic to determine what actions to take including: scan for threats; block or allow traffic; logging; and packet marking.

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

Both when the TOE receives data from the network and when it transmits data to the network, it ensures that the buffers are not padded out with previously transmitted or otherwise residual information.

The TSF relies on the domain controller in the IT environment, which is used with the User Identification Agent, to provide it with user specific information that is used in policies and reporting.

2.2.2.4 Identification and Authentication

The TOE ensures that all users accessing the TOE user interfaces are identified and authenticated. The TOE accomplishes this by supporting local user authentication using an internal database. The TOE maintains information that includes username, password, and role (set of privileges), which it uses to authenticate the human user and to associate that user with an authorized role. In addition, the TOE can be configured to lock a user out after a configurable number of unsuccessful authentication attempts.

2.2.2.5 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, configure the audit function including selection of the auditable events, configure the information flow control rules, and review the audit trail. The TOE provides Security Administrator, Audit Administrator, and Cryptographic Administrator and ensures the appropriate functions are restricted to these roles and there is no overlap between the roles, except that all administrators have read access to the audit trail.

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

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

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

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

2.2.2.7 Resource Utilization

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

2.2.2.8 TOE Access

The TOE provides the capabilities for both TOE- and user-initiated locking of interactive sessions and for TOE termination of an interactive session after a period of inactivity. The TOE will display an advisory and consent warning message regarding unauthorized use of the TOE before establishing a user session. The TOE can also deny establishment of an authorized user session based on location, day, and time.

2.2.2.9 Trusted Path/Channels

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

2.2.3 Product Capabilities not supported in the TOE

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

Other items excluded from the TOE:

- Command Line Interface (CLI) management via Telnet or SSH (SCP is also excluded). Command Line Interface (CLI) access via SSH is restricted to the Superuser role (system admin) for maintenance and debugging purposes, which is outside normal operation of the TOE.
- HTTP web-based management
- Console Port
- USB Ports
- Dynamic role administrator accounts. The Superuser dynamic role may only be used for initial configuration and must otherwise be excluded from administration of the TOE. The device administrator, device administrator (read-only), virtual system administrator, virtual system administrator (read-only), and superuser (read-only) administrator roles may not be used in the evaluated configuration
- Custom admin roles. The device comes preconfigured with three custom admin roles. One for the Security Administrator, one for the Crypto Administrator, and one for the Audit Administrator. Additional custom admin roles must not be created and used to determine access levels for administrators.
- Tap Mode (Interface mode in which traffic may only be observed and not secured)
- Kerberos – For authentication of administrators
- Custom Applications and custom definition methods – Administrators may define custom applications in order to identify and control their own internally developed applications
- NTP – To set the system's time
- Captive
- Portal – Used to identify users when they do not authenticate to Active Directory
- GlobalProtect – VPN capability for remote users; this is a separately licensed feature
- HIP Profiles – Part of the GlobalProtect feature set used to verify the host's configuration prior to granting access
- SSL-VPN – VPN capability for remote users
- Terminal Services Agent – This is a separate software image used when terminal services are required along with user identification
- REST API – An API used to perform select configuration and administration tasks on the firewall; the REST API is available only to administrators with Superuser accounts and is therefore not permitted in Common Criteria mode
- User-ID XML API – An API used to provide user to IP mappings to the firewall
- Log Forwarding – using FTP and TFTP
- RADIUS – For administrator authentication
- SSHv1 – Disabled in Common Criteria mode
- The authentication methods (e.g., CHAP/PAP) for PPPoE
- The eDirectory

- The tunnel monitoring
- SSLv1, SSLv2, SSLv3 – Disabled in Common Criteria mode
- DNS – Not required to enforce any SFRs; MRPP section 2.3 states – "Remote administration is a required information flow to the TOE, authentication/certificate servers, Network Time Protocol (NTP) servers, as well as any other IT entities are optional."
- Software Update – The TOE system software must not be updated in order to maintain CC compliance
- Active/active HA pairs
- Botnet and country based policy enforcement
- URL Category in Match Criteria - The default setting for the URL Category for the Security Policy Rule is "Any". The user should retain the default setting and should not select a URL Category from the pull down menu.
- WildFire – The file blocking profile action list includes a "forward" action, which will copy and forward files matching the policy to the WildFire cloud-based malware detection service. This is disallowed in the TOE. Wildfire is a separately licensed feature.
- SHA-2 VPN Support – The cryptographic hashing services using SHA-1 in support of the TOE's VPN capability can be manually selected.
- The internal User-ID Agent - The external, separately installed UIA is included and will be required to be used in the evaluated configuration as it was in the original evaluation.
- IPv6 Support for User-ID
- Palo Alto Networks URL Filtering Database (PAN-DB) - The use of Brightcloud is still supported and will be required for use in the TOE.
- IP Based Threat Exceptions
- Dynamic Block List
- WildFire Subscription Service
- Decryption Control – A new Decryption Profile has been introduced with several options to provide better control over SSL and SSH sessions. These additional Decryption Profile options have not been subject to evaluation.
- HA2 Keep-alive – When configuring HA, you can enable monitoring on the HA2 data link between HA peers. This feature is excluded and should not be enabled in the evaluated configuration.
- HA Path Monitoring Update - This feature is excluded and should not be enabled in the evaluated configuration. The default values should be applied.
- HA IPv6 Support – HA control and data link support and IPv6 HA path monitoring is available. This feature is excluded and should not be enabled in the evaluated configuration. The default values should be applied.
- Dataplane Health Monitoring – The PA-5000 Series and PA-3000 Series devices support an internal dataplane health monitor that will continually monitor all of the components of the dataplane. This feature is excluded and should be disabled in the evaluated configuration.
- Virtual Wire Subinterface – User can create virtual wire subinterfaces in order to classify traffic into different zones and virtual systems. This feature is excluded and should not be enabled in the evaluated configuration.
- Bad IP Option Protection – In zone protection profiles, user can now specify options to drop packets with non-conformant IP options. This feature is excluded and should not be enabled in the evaluated configuration.

- SLAAC – Stateless Address Autoconfiguration (SLAAC) is now supported on IPv6-configured interfaces. This feature is excluded and should not be enabled in the evaluated configuration.
- IPv6 over IPSec – This feature enables routing of IPv6 traffic over an IPSec tunnel established between IPv4 endpoints. This feature is excluded and should not be enabled in the evaluated configuration.
- NAT64 – NAT64 enables the firewall to translate source and destination IP headers between IPv6 and IPv4. This feature is excluded and should not be enabled in the evaluated configuration.
- Minimum Password Complexity – Allows you to define a set of password requirements that all local administrator accounts must adhere to, such as minimum length, minimum lower and upper case letters, requirement to include numbers or special characters, ability to block repeated characters and set password change periods. This feature is excluded and should not be enabled in the evaluated configuration.
- IPv6 Management Services - This feature is excluded in the TOE and the user should not configure them in the evaluated configuration.
- The OCSP responder is a means of predefining an additional field used during certificate generation. It does not need to be configured and is excluded in the TOE.
- Shutdown Device feature allows sessions to be logged prior to a shutdown is excluded in the TOE and the user should not use it in the evaluated configuration.
- Support for HSM is a new feature that is excluded in the TOE. Use of this feature requires a component in the operating environment that is not included in the evaluated configuration.
- The Option to Disable SIP ALG is a new feature that is excluded in the TOE. The users are instructed not to disable SIP ALG.
- TLS 1.2 Decryption is a new feature that is excluded in the TOE and has not been subject to evaluation.
- The User-ID Integration with Syslog as excluded in the TOE.
- The extended-capture option in the Threat Detection settings is excluded and the users are instructed not to configure extended-capture.
- URL Filtering Search Engine Cached Site Enhancement - This new feature enhancement is excluded in the TOE as it has not been covered in the scope of the evaluation.
- URL Filtering Translation Site Filtering Enhancement - This new feature enhancement is excluded in the TOE as it has not been covered in the scope of the evaluation.
- URL Safe Search Enforcement is a new feature that is excluded in the TOE. By default it is disabled. IKE PKI Certificate Authentication for IPsec Site to Site VPNs is a new feature that is excluded in the TOE.
- Content Delivery Network (CDN)/Update Server Verification - This new feature is excluded in the TOE. The users are instructed not to check the “Verify Update Server Identity check box in the Services dialog”.
- Support for Color-Coded Tags - This new feature is excluded in the TOE. The users are instructed not to configure tags via the Objects >Tags tab.
- The Virtual Machine Monitoring Agent is excluded in the TOE and the users are instructed not to configure VM information sources.
- Dynamic Address Groups are excluded in the TOE the users are instructed not to configure them.
- URL Safe Search Enforcement is a new feature that is excluded in the TOE. By default it is disabled. The users are instructed not to enable this option.

2.3 TOE Documentation

Palo Alto Networks Inc. offers a series of documents that describe the installation of Palo Alto Networks next-generation firewalls as well as guidance for subsequent use and administration of the applicable security features. These documents include:

- Palo Alto Networks Web Interface Reference Guide, Release 6.0
- PAN-OS Command Line Interface Reference Guide, Release 6.0

The support service accounts are required for an additional service fee in order to obtain information about bug fixes included in the release notes.

3. Security Problem Definition

This section describes the threats to assets the TOE is intended to counter, the organizational security policies the TOE is required to enforce, and assumptions about the operational environment and method of use of the TOE. The assumptions, threats, and organizational security policies are reproduced from the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, July 25, 2007. Exceptions are notated with an asterisk. Refer to Section 7, which provides the rationale for all changes, additions and modifications to the MRPP.

3.1 Assumptions

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

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

3.2 Threats

The following threats are to be countered by the TOE:

T.ADDRESS_MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TSF data being compromised.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.CRYPTO_COMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.
T.MASQUERADE	A user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.

T.FLAWED_IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered.
T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.RESOURCE_EXHAUSTION	A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.
T.SPOOFING	An entity may misrepresent itself as the TOE to obtain authentication data.
T.MALICIOUS_TSF_ COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user may gain access to services (by sending data through or to the TOE) for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

3.3 Organizational Security Policies

The following organizational security policies are to be satisfied by the TOE:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signature operations.
P.CRYPTOGRAPHY_VALIDATED	Where the TOE requires FIPS-approved security functions, only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).

P.VULNERABILITY_ANALYSIS_TEST	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

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 U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, July 25, 2007. Exceptions are notated with an asterisk. Refer to Section 7, which provides the rationale for all changes, additions and modifications to the MRPP.

4.1 Security Objectives for the TOE

This section defines the security objectives that are to be addressed by the TOE.

O.ROBUST_ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure delivery and management.
O.ADMIN_ROLE	The TOE will provide an administrator role to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.
O.CHANGE_MANAGEMENT	The configuration of, and all changes to, the TOE and its development evidence will be analyzed, tracked, and controlled throughout the TOE's development.
O.CORRECT_ TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF in its operational environment.
O.CRYPTOGRAPHIC_ FUNCTIONS	The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signature operations.
O.CRYPTOGRAPHY_ VALIDATED	The TOE shall use NIST FIPS 140-2 validated crypto modules for cryptographic services implementing FIPS-approved security functions and random number generation services used by cryptographic functions.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.THOROUGH_FUNCTIONAL_ TESTING	The TOE will undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.
O.MAINT_MODE	The TOE shall provide a mode from which recovery or initial startup procedures can be performed.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.

O.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of TSF data and security attributes.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.
O.RESOURCE_SHARING	The TOE shall provide mechanisms that mitigate attempts to exhaust connection-oriented resources provided by the TOE (e.g., entries in a connection state table; Transmission Control Protocol (TCP) connections used by proxies).
O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.
O.SOUND_IMPLEMENTATION	The implementation of the TOE will be an accurate instantiation of its design, and is adequately and accurately documented.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.TRUSTED_PATH	The TOE will provide a means to ensure administrators are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.
O.VULNERABILITY_ANALYSIS_TEST	The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with medium attack potential to violate the TOE's security policies.

4.2 Security Objectives for the Operating Environment

This section defines the security objectives that are to be addressed by the operational environment of the TOE.

OE.CRYPTANALYTIC	Cryptographic methods used in the IT environment shall be interoperable with the TOE, should be FIPS 140-2 validated and should be resistant to cryptanalytic attacks (i.e., will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).
OE.NO_GENERAL_PURPOSE	The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
*OE.UIA_ONLY	The PC used for the UIA component is dedicated to this function and is not used for any other purpose.

5. IT Security Requirements

This section specifies the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for the TOE. The requirements in this section have been drawn from the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, July 25, 2007 and from the Common Criteria.

5.1 Extended Component Definitions

The following extended security requirements are identified in this Security Target:

- FAU_ARP_ACK_(EXT).1: Security alarm acknowledgement
- FCS_BCM_(EXT).1: Baseline cryptographic module
- FCS_CKM_(EXT).2: Cryptographic key handling and storage
- FCS_COP_(EXT).1: Random number generation
- FIA_UAU_(EXT).2: Specified user authentication before any action
- FIA_UAU_(EXT).5: Authentication mechanism
- FPT_TST_(EXT).1: TSF testing

All of these requirements are defined in the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments.

The U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments also includes NIAP-interpreted SFRs. Although it is unclear these constitute extended components as defined by the CC, they are categorized as such in the PP. These additional requirements are:

- FAU_GEN.1-NIAP-0410: Audit data generation
- FAU_GEN.2-NIAP-0410: User identity association
- FAU_SAA.1-NIAP-0407: Potential violation analysis
- FAU_SEL.1.1-NIAP-0407: Selective audit
- FAU_STG.NIAP-0414-1-NIAP-0429: Site-configurable prevention of audit loss
- FMT_MSA.3-NIAP-0409: Static attribute initialization.

5.2 TOE Security Functional Requirements

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

Note that Section 7 provides the rationale for all modifications to the MRPP. The exceptions to the MRPP, including removed SFRs, modified SFRs, and additional SFRs are notated with an asterisk.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_ARP.1: Security alarms
	FAU_ARP_ACK_(EXT).1: Security alarm acknowledgement
	FAU_GEN.1-NIAP-0410: Audit data generation
	FAU_GEN.2-NIAP-0410: User identity association
	FAU_SAA.1-NIAP-0407: Potential violation analysis

Requirement Class	Requirement Component
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_SAR.3: Selectable audit review
	FAU_SEL.1-NIAP-0407: Selective audit
	FAU_STG.1: Protected audit trail storage
	FAU_STG.3: Action in case of possible audit data loss
	FAU_STG.NIAP-0414-1-NIAP-0429: Site-configurable prevention of audit loss
FCS: Cryptographic support	FCS_BCM_(EXT).1: Basic cryptographic module
	FCS_CKM.1(1): Cryptographic key generation (for symmetric keys)
	FCS_CKM.1(2): Cryptographic key generation (for asymmetric keys)
	FCS_CKM.2: Cryptographic key distribution
	FCS_CKM_(EXT).2: Cryptographic key handling and storage
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1(1): Cryptographic operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic operation (cryptographic signature)
	FCS_COP.1(3): Cryptographic operation (cryptographic hashing)
	FCS_COP.1(4): Cryptographic operation (for cryptographic key agreement)
	FCS_COP.1(5): Cryptographic operation (for SHA-1)
	FCS_COP_(EXT).1: Random number generation
FDP: User Data Protection	FDP_IFC.1(1): Subset information flow control (unauthenticated policy)
	FDP_IFC.1(2): Subset information flow control (unauthenticated TOE services policy)
	FDP_IFC.1(3): Subset information flow control (VPN policy)
	FDP_IFF.1(1): Simple security attributes (unauthenticated policy)
	FDP_IFF.1(2): Simple security attributes (unauthenticated TOE services policy)
	FDP_IFF.1(3): Simple security attributes (VPN policy)
	FDP_RIP.2: Full 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_UAU_(EXT).2: Specified user authentication before any action
	FIA_UAU_(EXT).5: Authentication mechanism
	FIA_UID.2: User authentication before any action
	FIA_USB.1: User-subject binding

Requirement Class	Requirement Component
FMT: Security Management	FMT_MOF.1(1): Management of security functions behavior (TSF non-cryptographic self test)
	FMT_MOF.1(2): Management of security functions behavior (Cryptographic self test)
	FMT_MOF.1(3): Management of security functions behavior (audit and alarms)
	FMT_MOF.1(4): Management of security functions behavior (audit and alarms)
	FMT_MOF.1(5): Management of security functions behavior (audit and alarms)
	FMT_MOF.1(6): Management of security functions behavior (available TOE services for unauthenticated users)
	FMT_MOF.1(7): Management of security functions behavior (quota mechanism)
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3-NIAP-0409(1): Static attribute initialization
	FMT_MSA.3-NIAP-0409(2): Static attribute initialization
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1(1): Management of TSF data (non-cryptographic, non-time TSF data)
	FMT_MTD.1(2): Management of TSF data (cryptographic TSF data)
	FMT_MTD.1(3): Management of TSF data (time TSF data)
	FMT_MTD.1(4): Management of TSF data (information flow policy ruleset)
	FMT_MTD.1(5): Management of TSF data (network interfaces)
	FMT_MTD.2(1): Management of limits on TSF data (transport-layer quotas)
	FMT_MTD.2(2): Management of limits on TSF data (controlled connection-oriented quotas)
	FMT_REV.1: Revocation
	FMT_SMR.2: Restrictions on security roles
FPT: Protection of the TSF	FPT_FLS.1: Failure with preservation of security state
	FPT_ITC.1: Inter-TSF confidentiality during transmission
	FPT_ITT.1: Basic internal TSF data transfer
	FPT_RCV.1: Manual recovery
	FPT_RPL.1: Replay detection
	FPT_STM.1: Reliable time stamps
	FPT_TST_(EXT).1: TSF testing
	FPT_TST.1(1): TSF testing (for cryptography)
	FPT_TST.1(2): TSF testing (for key generation components)

Requirement Class	Requirement Component
FRU: Resource Utilisation	FRU_FLT.1: Degraded fault tolerance
	FRU_RSA.1(1): Maximum quotas (transport-layer quotas)
	FRU_RSA.1(2): Maximum quotas (controlled connection-oriented quotas)
FTA: TOE Access	FTA_SSL.2: User initiated locking
	FTA_SSL.3: TSF-initiated termination
	FTA_TAB.1: Default TOE access banners
	FTA_TSE.1: TOE session establishment
FTP: Trusted Path/Channels	FTP_ITC.1(1): Inter-TSF trusted channel (Prevention of disclosure)
	FTP_ITC.1(2): Inter-TSF trusted channel (Detection of modification)
	FTP_TRP.1(1): Trusted path (Prevention of disclosure)
	FTP_TRP.1(2): Trusted path (Detection of modification)

Table 1: TOE Security Functional Requirements

5.2.1 Security Audit

5.2.1.1 Security alarms (FAU_ARP.1)

FAU_ARP.1.1 The TSF shall immediately display an alarm message, identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) that generated the alarm, at the:

- local console,
- remote administrator sessions that exist, and;
- remote administrator sessions that are initiated before the alarm has been acknowledged, and;
- at the option of the Security Administrator, generate an audible alarm, and;
- **[no other methods]**

upon detection of a potential security violation.

5.2.1.2 Extended: Security alarm acknowledgement (FAU_ARP_ACK_(EXT).1)

FAU_ARP_ACK_(EXT).1.1 The TSF shall display the alarm message identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) until it has been acknowledged. An audible alarm will sound until acknowledged by an administrator.

FAU_ARP_ACK_(EXT).1.2 The TSF shall display an acknowledgement message identifying a reference to the potential security violation, a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm, at the:

- local console, and
- remote administrator sessions that received the alarm.

5.2.1.3 Audit Data Generation (FAU_GEN.1-NIAP-0410)

FAU_GEN.1.1-NIAP-0410 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 auditable events listed in Table ~~3~~ **2**;

c) **[*events at a basic level of audit introduced by the inclusion of additional SFRs*]**.

FAU_GEN.1.2-NIAP-0410 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subjects identity (if applicable), and the 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 three of Table ~~3~~ **2** below.

Requirement	**Auditable Events**	**Additional Audit Record Contents**
FAU_ARP.1	Potential security violation was detected	Identification of what caused the generation of the alarm
FAU_ARP_ACK_(EXT).1*	~~None~~ **Acknowledgement of alarm.**	The identity of the administrator that acknowledged the alarm.
FAU_GEN.1-NIAP-0410	None	
FAU_GEN.2-NIAP-0410	None	
FAU_SAA.1-NIAP-0407	Enabling and disabling of any of the analysis mechanisms	The identity of the Security Administrator performing the function
FAU_SAR.1	Opening the audit trail	The identity of the Administrator performing the function
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	The identity of the administrator performing the function
FAU_SAR.3	None	
FAU_SEL.1-NIAP-0407	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Security Administrator performing the function
FAU_STG.1	None	
FAU_STG.3	Actions taken due to exceeding the audit threshold	The identity of the Security Administrator performing the function
FAU_STG.NIAP-0414-1-NIAP-0429	Actions taken due to the audit storage failure	The identity of the Security Administrator performing the function
FCS_BCM_(EXT).1	None	
FCS_CKM_EXT.2	Failure of the Cryptographic Key Handling and Storage	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1(1)	Failure of the symmetric key generation	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_CKM.1(2)	Failure of the asymmetric key generation	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_CKM.2	Failure of the Key distribution	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_CKM.4	Failure of the Key destruction	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_COP.1(1)	Failure of cryptographic operation (for data encryption/decryption)	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_COP.1(2)	Failure of cryptographic operation (for cryptographic signature)	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_COP.EXP.1	Failure of cryptographic operation (Random Number generation)	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_COP.1(3)	Failure of cryptographic operation (for cryptographic hashing)	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FCS_COP.1(4)	Failure of cryptographic operation (for cryptographic key Agreement)	**Type of cryptographic operation** **Any applicable cryptographic mode(s) of operation, excluding any sensitive information**

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1(5)*	**Failure of cryptographic operation (for cryptographic hashing)**	**Type of cryptographic operation** **Any applicable cryptographic mode(s) of operation, excluding any sensitive information**
FDP_IFC.1(1)	None	
FDP_IFC.1(2)	None	
FDP_IFC.1(3)*	**None**	
FDP_IFF.1(1)	Decisions to permit/deny information flows	Presumed identity of source subject Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow
FDP_IFF.1(2)	Decisions to permit/deny information flows between a subject and the TOE	Presumed identity of source subject Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow, if applicable[1]

[1] The TOE may not use a rule in a ruleset to allow/disallow TOE services (e.g., configuration parameter could be used instead) and if this is the case, it is not required that a rule be identified.

Requirement	Auditable Events	Additional Audit Record Contents
FDP_IFF.1(3)*	**Decisions to permit/deny information flows**	**Presumed identity of source subject** **Identity of destination subject** **Transport layer protocol, if applicable** **Source subject service identifier, if applicable** **Destination subject service identifier, if applicable** **Identity of the firewall interface on which the TOE received the packet** **For denied information flows, the reason for denial**
FDP_RIP.2	None	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts The actions (e.g. disabling of an account) taken The subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of an account)	Identity of the unsuccessfully authenticated user
FIA_ATD.1	None	
FIA_UAU.1	None	
FIA_UAU_(EXT).2	Successful and unsuccessful use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UAU_(EXT).5	All use of the local authentication mechanism	Claimed identity of the user attempting to authenticate
FIA_UID.2	All use of the user identification mechanism used for authorized users (that is, those that authenticate to the TOE)	Claimed identity of the user using the identification mechanism
FIA_USB.1	Success and failure of binding of user security attributes to a subject	The identity of the user whose attributes are attempting to be bound
FMT_MOF.1(1)	All modifications in the behavior of the functions in the TSF	The identity of the administrator performing the function
FMT_MOF.1(2)	Enabling or disabling of the key-generation self-tests	The identity of the administrator performing the function
FMT_MOF.1(3)	All modifications in the behavior of the functions in the TSF	The identity of the administrator performing the function
FMT_MSA.1	All manipulation of the security attributes	The identity of the administrator performing the function

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MSA.3-NIAP-0409(1)	None	
FMT_MSA.3-NIAP-0409(2)	None	
FMT_MSA.3*	**Modifications of the default setting of permissive or restrictive rules** **All modifications of the initial values of security attributes**	**The identity of the administrator performing the function**
FMT_MTD.1(1)*	All modifications of the user name, password and role of ~~TSF data~~ **administrator roles and administrative users** by the administrator	The identity of the administrator performing the function
FMT_MTD.1(2)	All modifications of the values of cryptographic security data by the cryptographic administrator	The identity of the administrator performing the function
FMT_MTD.1(3)	All modifications to the time and date used to form the time stamps by the administrator	The identity of the administrator performing the function
FMT_MTD.1(4)	All modifications to the information flow policy ruleset by the Security Administrator	The identity of the security administrator performing the function
FMT_MTD.1(5)	All modifications of network interface configurations by the administrator	The identity of the security administrator performing the function
FMT_MTD.2(1)	All modifications of the limits Actions taken when the quota is exceed**ed** (includ**ing** the fact that the quota was exceeded)	The identity of the administrator performing the function
FMT_MTD.2(2)	All modifications of the limits Actions taken when the quota is exceed**ed** (includ**ing** the fact that the quota was exceeded)	The identity of the administrator performing the function
FMT_REV.1	All attempts to revoke security attributes	List of security attributes that were attempted to be revoked The identity of the administrator performing the function
FMT_SMR.2	Modifications to the group of users that are part of a role	User IDs that are associated with the modifications The identity of the administrator performing the function
FPT_FLS.1*	**Failure of the TSF**	**Type of failure**
FPT_ITC.1*	**None**	
FPT_ITT.1*	**None**	
FPT_RCV.1	The fact that a failure or service discontinuity occurred Resumption of the regular operation	Type of failure or service discontinuity

Requirement	Auditable Events	Additional Audit Record Contents
FPT_RPL.1	Notification that a replay event occurred	Identity of the user that was the subject of the replay attack
FPT_STM.1	Changes to the time	The identity of the administrator performing the function
FPT_TST_(EXT).1	Execution of this set of TSF self tests	The identity of the administrator performing the test, if initiated by an administrator
FPT_TST.1(1)	Execution of this set of TSF self tests (for cryptography)	The identity of the administrator performing the test, if initiated by an administrator
FPT_TST.1(2)	Execution of this set of TSF self tests (for key generation components)	The identity of the administrator performing the test, if initiated by an administrator
FRU_FLT.1*	**All TOE capabilities being discontinued due to a failure**	**TOE capability being discontinued** **Type of failure**
FRU_RSA.1(1)	None	
FRU_RSA.1(2)	None	
~~FTA_SSL.1~~*	~~Locking of an interactive session by the session locking mechanism~~ ~~Any attempts at unlocking of an interactive session~~	~~The identity of the user associated with the session being locked or unlocked~~
FTA_SSL.2	Locking of an interactive session by the session locking mechanism Any attempts at unlocking of an interactive session	The identity of the user associated with the session being locked or unlocked
FTA_SSL.3	The termination of a remote session by the session locking mechanism	The identity of the user associated with the session that was terminated
FTA_TAB.1	None	
FTA_TSE.1	All attempts at establishment of a user session	The identity of the user attempting to establish the session For unsuccessful attempts, the reason for denial of the establishment attempt
FTP_ITC.1(1)	All attempted uses of the trusted channel functions	Identification of the initiator and target of all trusted channels
FTP_ITC.1(2)	All attempted uses of the trusted channel functions	Identification of the initiator and target of all trusted channels

Requirement	Auditable Events	Additional Audit Record Contents
FTP_TRP.1(1)	All attempted uses of the trusted path functions	Identification of the claimed user identity
FTP_TRP.1(2)	All attempted uses of the trusted path functions	Identification of the claimed user identity

Table 2: Audit Events

5.2.1.4 User identity association (FAU_GEN.2-NIAP-0410)

FAU_GEN.2.1-NIAP-0410 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.5 Potential violation analysis (FAU_SAA.1-NIAP-0407)

FAU_SAA.1.1-NIAP-0407 The TSF shall be able to apply a set of rules in monitoring events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2-NIAP-0407* The TSF shall enforce the following rules for monitoring events:

a) Security Administrator specified number of authentication failures;

b) Security Administrator specified number of Information Flow policy violations by an individual presumed source network identifier (e.g., IP address) within an administrator specified time period;

c) Security Administrator specified number of Information Flow policy violations to an individual destination network identifier within an administrator specified time period;

d) Security Administrator specified number of Information Flow policy violations to an individual destination subject service identifier (e.g., TCP port) within an administrator specified time period;

e) Security Administrator specified Information Flow policy rule, or group of rule violations within an administrator specified time period;

f) Any detected replay of TSF data or security attributes;

g) Any failure of the cryptomodule self-tests;

h) Any failure of the other TSF self-tests;

i) Security Administrator specified number of encryption/decryption failures;

~~j) Security Administrator specified number of decryption failures;~~

k) **[*no additional rules*]**;

known to indicate a potential security violation.

5.2.1.6 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide the Administrators with the capability to read all audit data from the audit records.

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

5.2.1.7 Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records in the audit trail, except the Administrators.

5.2.1.8 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) user identity;
b) source subject identity;
c) destination subject identity;
d) ranges of one or more: dates, times, user identities, subject service identifiers, or transport layer protocol;
e) rule identity;
f) TOE network interfaces; and
g) **[*no additional criteria*]**.

5.2.1.9 Selective audit (FAU_SEL.1-NIAP-0407)

FAU_SEL.1.1-NIAP-0407 The TSF shall allow only the Security Administrator to include or exclude auditable events from the set of audited events based on the following attributes:

a) user identity;
b) event type;
c) network identifier;
d) subject service identifier;
e) success of auditable security events;
f) failure of auditable security events;
g) rule identity; and
h) **[*no additional criteria*]**.

5.2.1.10 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall restrict the deletion of stored audit records in the audit trail to the Audit Administrator.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the stored audit records in the audit trail.

5.2.1.11 Action in case of possible audit data loss (FAU_STG.3)

FAU_STG.3.1 The TSF shall immediately alert the administrators by displaying a message at the local console, and at the remote administrative console when an administrative session exists for each of the defined administrative roles, at the option of the Security Administrator generate an audible alarm, **[*no other methods*]** if the audit trail exceeds a Security Administrator settable percentage of storage capacity.

5.2.1.12 Site-Configurable Prevention of Audit Loss (FAU_STG.NIAP-0414-1-NIAP-0429)

FAU_STG.NIAP-0414-1.1-NIAP-0429 The TSF shall provide the Security Administrator the capability to select one or more of the following actions**:** prevent auditable events, except those taken by the Security Administrator and Audit Administrator, overwrite the oldest stored audit records and **[*no other actions*]** to be taken if the audit trail is full.

FAU_STG.NIAP-0414-1.2-NIAP-0429 The TSF shall enforce the Security Administrator's selection(s) if the audit trail is full.

5.2.2 Cryptographic Support

5.2.2.1 Baseline cryptographic module (FCS_BCM_(EXT).1)

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_(EXT).1.2 All cryptographic modules implemented in the TOE **[*(3) As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.*]**

5.2.2.2 Cryptographic key generation (for symmetric keys) (FCS_CKM.1(1))

FCS_CKM.1.1(1) The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

5.2.2.3 Cryptographic key generation (for asymmetric keys) (FCS_CKM.1(2))

FCS_CKM.1.1(2) The TSF shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard **[ANSI X9.31 algorithm]**, using a domain parameter generator and **[*(1) a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1*]** in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 128 bits using conservative estimates.

5.2.2.4 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[*(1) Manual (Physical) Method, and (2) Automated (Electronic) Method*]** that meets the following:

- NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

5.2.2.5 Cryptographic key handling and storage (FCS_CKM_(EXT).2)

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(EXT).2.3* The TSF shall destroy non-persistent cryptographic keys ~~after a cryptographic administrator-defined period of time of inactivity~~ **as soon as their associated sessions end**.

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

5.2.2.6 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key zeroization requirements of FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

5.2.2.7 Cryptographic operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1.1(1) The cryptomodule shall perform encryption and decryption using the FIPS-approved security function AES algorithm operating in **[CBC, ECB, or CTR mode]** and cryptographic key size of **[*128 bits, 192 bits, 256 bits*]**.

5.2.2.8 Cryptographic operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services using the FIPS-approved security function **[*(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of [2048 bits or 3072 bits]*]** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

5.2.2.9 Cryptographic operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of **[*256 bits, 384 bits, 512 bits*]**.

5.2.2.10 Cryptographic operation (for cryptographic key agreement) (FCS_COP.1(4))

FCS_COP.1.1(4) The TSF shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" **[*(1) [Diffie-Hellman] and cryptographic key sizes (modulus) of [2048 bits]*]** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

5.2.2.11 Cryptographic operation (for SHA-1) (FCS_COP.1(5))

FCS_COP.1.1(5)* The TSF shall perform **[cryptographic hashing]** in accordance with a specified cryptographic algorithm **[SHA-1]** and cryptographic ~~key~~ **hash** sizes **[160 bits]** that meet the following: **[FIPS 180-3].**

5.2.2.12 Random number generation (FCS_COP_(EXT).1)

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG

) services in accordance with a FIPS-approved RNG **[ANSI X9.31 algorithm]** seeded by **[*(3) a combination of hardware-based and software-based entropy sources.*]**

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

5.2.3 User Data Protection

5.2.3.1 Subset information flow control (unauthenticated policy) (FDP_IFC.1(1))

FDP_IFC.1.1(1) The TSF shall enforce the UNAUTHENTICATED INFORMATION FLOW SFP on

- source subject: TOE interface on which information is received;
- destination subject: TOE interface to which information is destined;
- information: network packets; and
- operations: pass information.

5.2.3.2 Simple security attributes (unauthenticated policy) (FDP_IFF.1(1))

FDP_IFF.1.1(1) The TSF shall enforce the UNAUTHENTICATED INFORMATION FLOW SFP based on at least the following types of subject and information security attributes:

a) Source subject security attributes:
- Set of source subject identifiers; and
- **[*none*]**.

b) Destination subject security attributes:
- Set of destination subject identifiers; and
- **[*none*]**.

c) Information security attributes:
- presumed identity of source subject;
- identity of destination subject;
- transport layer protocol
- source subject service identifier;
- destination subject service identifier (e.g., TCP or UDP destination port number);
- **[*[source and destination security zones;***
- ***user;***
- ***application (Traffic payload)]***].
- Stateful packet attributes: **[*for IP-based network stacks:***
  - ***Connection-oriented protocols:***
    - ***sequence number;***
    - ***acknowledgement number;***
    - ***Flags:***
      - ***SYN;***
      - ***ACK;***
      - ***RST;***
      - ***FIN; and***
    - ***[none].***
  - ***Connectionless protocols:***
    - ***Source and destination network identifiers;***
    - ***Source and destination service identifiers;***
    - ***[none]***].

FDP_IFF.1.2(1)* The TSF shall permit an information flow between a source subject and a destination subject via a controlled operation if the following rules hold:

- the presumed identity of the source subject is in the set of source subject identifiers;
- the identity of the destination subject is in the set of ~~source~~ destination **subject** identifiers;
- the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by the Security Administrator) according to the following algorithm

[If the packet represents a new connection, sequentially search the ordered policy ruleset for a policy that matches the source and destination zones. If a policy that allows traffic between the zones is found, perform application identification. Otherwise, drop the packet.

Once the application is identified, sequentially search the ordered policy ruleset for a policy that matches all the information security attributes. The first matching policy rule found is applied. If it allows the traffic, a session is created and additional checks are made for matching NAT, SSL, SSH Decryption, and Application Override policy rules. In addition, any security profiles identified in the matching policy rule are applied—these comprise Antivirus, Antispyware, Vulnerability Protection, File Blocking, URL Filtering, and Data Filtering. Otherwise, if the matching policy rule denies the traffic, or no matching rule is found, the packet is dropped.

Packets that are part of an existing session are processed against applicable security profiles]; and

- the selected information flow policy rule specifies that the information flow is to be permitted.

FDP_IFF.1.3(1) The TSF shall enforce the following:

- fragmentation rule:
  - prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets;
- stateful packet inspection rules:
  - whenever a packet is received that is not associated with an allowed established session (e.g., the SYN flag is set without the ACK flag being set), the information flow policy ruleset, as defined in FDP_IFF.1.2(1), is applied to the packet;
  - otherwise, the TSF associates a packet with an allowed established session using the stateful packet attributes.

FDP_IFF.1.4(1) The TSF shall provide the following**:** the Security Administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied.

FDP_IFF.1.5(1) The TSF shall explicitly authorize an information flow based on the following rules: none.

FDP_IFF.1.6(1) 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 presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;

c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;

d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.

5.2.3.3 Subset information flow control (unauthenticated TOE services policy) (FDP_IFC.1(2))

FDP_IFC.1.1(2) The TSF shall enforce the UNAUTHENTICATED TOE SERVICES SFP on

- source subject: TOE interface on which information is received;
- destination subject: the TOE;
- information: network packets; and
- operations: accept or reject network packet.

5.2.3.4 Simple security attributes (unauthenticated TOE services policy) (FDP_IFF.1(2))

FDP_IFF.1.1(2) The TSF shall enforce the UNAUTHENTICATED TOE SERVICES SFP based on the following types of subject and information security attributes:

a) Source subject security attributes:
- Set of source subject identifiers; and
- **[*none*].**

b) Destination subject security attributes:
- TOE's network identifier; and
- **[*none*].**

c) Information security attributes:
- presumed identity of source subject;
- identity of destination subject;
- transport layer protocol
- source subject service identifier;
- destination subject service identifier (e.g., TCP or UDP destination port number); and
- **[*for an IP-based network stack: ICMP message type and code as specified in RFC 792, [none]*]**.

FDP_IFF.1.2(2) The TSF shall permit an information flow between a source subject and the TOE via a controlled operation if the following rules hold:
- the presumed identity of the source subject is in the set of source subject identifiers;
- the identity of the destination subject is the TOE;
- the information security attributes match the attributes in an information flow control policy according to the following algorithm **[the first rule that matches the information security attributes is applied]**.

FDP_IFF.1.3(2) The TSF shall enforce the following rules:
- The TOE shall allow source subjects to access TOE services **[*for an IP-based network stack: ICMP, [SNMP]*]** without authenticating those source subjects; and
- The TOE shall allow the list of services specified immediately above to be enabled (become available to unauthenticated users) or disabled (become unavailable to unauthenticated users).

FDP_IFF.1.4(2) The TSF shall provide the following**:** the Security Administrator shall have the capability to view all information flows allowed by this information flow control policy before the policy is applied.

FDP_IFF.1.5(2) The TSF shall explicitly authorize an information flow based on the following rules: none.

FDP_IFF.1.6(2) The TSF shall explicitly deny an information flow based on the following rules:
- The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;
- The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;
- The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier; and
- The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the TOE.

5.2.3.5 Subset information flow control (VPN policy) (FDP_IFC.1(3))*

FDP_IFC.1.1(3) The TSF shall enforce the **[VPN SFP]** on **[**
- **source subject: TOE interface on which information is received;**
- **destination subject: TOE interface to which information is destined;**

- **information: network packets; and**
- **operations:**
  - **a) pass packets without modifying;**
  - **b) send IPSec encrypted and authenticated packets to a peer TOE using Encapsulating Security Payload (ESP) in tunnel mode**
  - c) **decrypt, verify authentication and pass received packets from a peer TOE in tunnel mode using ESP]**.

5.2.3.6 Simple security attributes (VPN policy) (FDP_IFF.1(3))*

FDP_IFF.1.1(3) The TSF shall enforce the **[VPN SFP]** based on the following types of subject and information security attributes: **[**

a) Source subject security attributes:
- **Set of source subject identifiers**

b) Destination subject security attributes:
- **Set of destination subject identifiers**

c) Information security attributes:
- **presumed identity of source subject;**
- **identity of destination subject]**.

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[**

- **the presumed identity of the source subject is in the set of source subject identifiers;**
- **the identity of the destination subject is in the set of destination subject identifiers]**.

FDP_IFF.1.3(1) The TSF shall enforce the **[no additional rules]**.

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: **[none]**.

FDP_IFF.1.5(1) 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 presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;**
- **b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;**
- **c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;**
- **d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject]**.

5.2.3.7 Full residual information protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[*allocation of the resource to*]** all objects.

5.2.4 Identification and Authentication

5.2.4.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when a Security Administrator-configurable integer of unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely and authorized IT entities.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall at the option of the Security Administrator prevent the remote administrators or authorized IT entity

from performing activities that require authentication until an action is taken by the Security Administrator, or until a Security Administrator defined time period has elapsed.

5.2.4.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to an authorized user:

a) user identifier(s):

- role;
- **[*[authentication data]*]**; and

b) **[*none*]**.

5.2.4.3 Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **[*for an IP-based network stack: ICMP [SNMP]*]** on behalf of the user to be performed before the user is authenticated.

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

5.2.4.4 Specified user authentication before any action (FIA_UAU_(EXT).2)

FIA_UAU_(EXT).2.1 The TSF shall require the administrators and authorized IT entities to be successfully authenticated before allowing any other TSF-mediated actions on behalf of these authorized users.

5.2.4.5 Authentication mechanism (FIA_UAU_(EXT).5)

FIA_UAU_(EXT).5.1 The TSF shall provide a local authentication mechanism, **[*[none]*]** to perform user authentication.

5.2.4.6 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.

5.2.4.7 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate all user security attributes with subjects acting on behalf of that authorized user.

5.2.5 Security Management

5.2.5.1 Management of security functions behavior (TSF non-cryptographic self-test) (FMT_MOF.1(1))

FMT_MOF.1.1(1) The TSF shall restrict the ability to modify the behavior of the functions TSF Self-test (FPT_TST_(EXT).1) to the Security Administrator.

5.2.5.2 Management of security functions behavior (Cryptographic self-test) (FMT_MOF.1(2))

FMT_MOF.1.1(2)* The TSF shall restrict the ability to enable, ~~disable~~ the functions TSF Self-test (FPT_TST.1(1), FPT_TST.1(2)) to the Cryptographic Administrator.

5.2.5.3 Management of security functions behavior (audit and alarms) (FMT_MOF.1(3))

FMT_MOF.1.1(3) The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions Security Audit (FAU_SAR) to an Administrator.

5.2.5.4 Management of security functions behavior (audit and alarms) (FMT_MOF.1(4))

FMT_MOF.1.1(4) The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions Security Audit Analysis (FAU_SAA); and Security Audit (FAU_SEL) to the Security Administrator.

5.2.5.5 Management of security functions behavior (audit and alarms) (FMT_MOF.1(5))

FMT_MOF.1.1(5) The TSF shall restrict the ability to enable, or disable the functions Security Alarms (FAU_ARP) to the Security Administrator.

5.2.5.6 Management of security functions behavior (available TOE-services for unauthenticated users) (FMT_MOF.1(6))

FMT_MOF.1.1(6) The TSF shall restrict the ability to enable, disable the functions **[*for an IP-based network stack: ICMP, [SNMP]*]** to the Security Administrator.

5.2.5.7 Management of security functions behavior (quota mechanism) (FMT_MOF.1(7))

FMT_MOF.1.1(7) The TSF shall restrict the ability to determine the behavior of the functions

- Controlled connection-oriented resource allocation (FRU_RSA.1(2));
- An administrator-specified network identifier;
- Set of administrator-specified network identifiers;
- Administrator-specified period of time

to the Security Administrator.

5.2.5.8 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1* The TSF shall enforce the UNAUTHENTICATED INFORMATION FLOW SFP, UNAUTHENTICATED TOE SERVICES SFP**, and VPN SFP** to restrict the ability to manipulate the security attributes referenced in the indicated policies to the Security Administrator.

5.2.5.9 Static attribute initialization (FMT_MSA.3-NIAP-0409(1))

FMT_MSA.3.1-NIAP-0409(1) The TSF shall enforce the UNAUTHENTICATED INFORMATION FLOW SFP to provide restrictive default values for the information flow policy ruleset that is used to enforce the SFP.

FMT_MSA.3.2-NIAP-0409(1) The TSF shall allow the Security Administrator to specify alternative initial values to override the default values when an object or information is created.

5.2.5.10 Static attribute initialization (FMT_MSA.3-NIAP-0409(2))

FMT_MSA.3.1-NIAP-0409(2) The TSF shall enforce the UNAUTHENTICATED TOE SERVICES SFP to provide restrictive default values for the set of TOE services available to unauthenticated users.

FMT_MSA.3.2-NIAP-0409(2) The TSF shall allow the Security Administrator to specify alternative initial values to override the default values when an object or information is created.

5.2.5.11 Static attribute initialization (FMT_MSA.3)*

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

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

5.2.5.12 Management of TSF data (non-cryptographic, non-time TSF data) (FMT_MTD.1(1))

FMT_MTD.1.1(1)* The TSF shall restrict the ability to **[*query, modify, delete, [[create]]*]** ~~all the TSF data except cryptographic security data and the time and date used to form the time stamps in FPT_STM.1~~ **administrator roles and administrative accounts** to the ~~administrators or authorized IT entities~~ **Security Administrator**.

5.2.5.13 Management of TSF data (cryptographic TSF data) (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to modify the cryptographic security data to the Cryptographic Administrator.

5.2.5.14 Management of TSF data (time TSF data) (FMT_MTD.1(3))

FMT_MTD.1.1(3)* The TSF shall restrict the ability to set the time and date used to form the time stamps in FPT_STM.1 to the Security Administrator.

5.2.5.15 Management of TSF data (Information flow policy ruleset) (FMT_MTD.1(4))

FMT_MTD.1.1(4) The TSF shall restrict the ability to query, modify, delete, create, ***[none]*** the information flow policy rules to the Security Administrator.

5.2.5.16 Management of TSF data (non-cryptographic, non-time TSF data) (FMT_MTD.1(5))

FMT_MTD.1.1(5)* The TSF shall restrict the ability to **[*query, modify*]** ~~all the TSF data except cryptographic security data and the time and date used to form the time stamps in FPT_STM.1~~ **network interfaces** to the ~~administrators or authorized IT entities~~ **Security Administrator**.

5.2.5.17 Management of limits on TSF data (transport-layer quotas) (FMT_MTD.2(1))

FMT_MTD.2.1(1) The TSF shall restrict the specification of the limits for quotas on transport-layer connections to the Security Administrator.

FMT_MTD.2.2(1) The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: **[block further transport-layer connections for the remainder of the configured time period]**.

5.2.5.18 Management of limits on TSF data (controlled connection-oriented quotas) (FMT_MTD.2(2))

FMT_MTD.2.1(2) The TSF shall restrict the specification of the limits for quotas on controlled connection-oriented resources to the Security Administrator.

FMT_MTD.2.2(2) The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: **[block further transport-layer connections for the remainder of the configured time period]**.

5.2.5.19 Revocation (FMT_REV.1)

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the users, information flow policy ruleset, services available to unauthenticated users, **[*none*]** within the TSC to the Security Administrator.

FMT_REV.1.2 The TSF shall immediately enforce the:

- revocation of a user's role (Security Administrator, Cryptographic Administrator, Audit Administrator);
- changes to the information flow policy ruleset when applied;
- disabling of a service available to unauthenticated users; and
- **[*none*]**.

5.2.5.20 Restrictions on security roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

- Security Administrator;
- Cryptographic Administrator (i.e., users authorized to perform cryptographic initialization and management functions);
- Audit Administrator; and
- **[*/None/*]**.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- All roles shall be able to administer the TOE locally;
- all roles shall be able to administer the TOE remotely;
- all roles are distinct; that is, there shall be no overlap of operations performed by each role, with the following exceptions:
- all administrators can review the audit trail; and
- all administrators can invoke the self-tests

are satisfied.

5.2.6 Protection of the TSF

5.2.6.1 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 link fails, or when one or more specified destinations cannot be reached by the active firewall]**.

5.2.6.2 Inter-TSF confidentiality during transmission (FPT_ITC.1)*

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

5.2.6.3 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.

5.2.6.4 Manual recovery (FPT_RCV.1)

FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

5.2.6.5 Replay detection (FPT_RPL.1)

FPT_RPL.1.1 The TSF shall detect replay for the following entities: TSF data and security attributes.

FPT_RPL.1.2 The TSF shall perform

- reject data;
- audit event; and
- **[*none*]**

when replay is detected.

5.2.6.6 Reliable time stamps (FPT_STM.1)

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

5.2.6.7 TSF testing (FPT_TST_(EXT).1)

FPT_TST_(EXT).1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_(EXT).1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

5.2.6.8 TSF testing (for cryptography) (FPT_TST.1(1))

FPT_TST.1.1(1) The TSF shall run a suite of self tests in accordance with FIPS PUB 140-2 and Appendix A of this ~~profile~~ **ST** during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions:

- key error detection;
- cryptographic algorithms;
- RNG/PRNG.

FPT_TST.1.2(1) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of TSF data related to the cryptography by using TSF-provided cryptographic functions.

FPT_TST.1.3(1) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions.

5.2.6.9 TSF testing (for key generation components) (FPT_TST.1(2))

FPT_TST.1.1(2) The TSF shall perform self-tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

FPT_TST.1.2(2) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of TSF data related to the key generation by using TSF-provided cryptographic functions.

FPT_TST.1.3(2) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

5.2.7 Resource Allocation

5.2.7.1 Degraded fault tolerance (FRU_FLT.1)*

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

5.2.7.2 Maximum quotas (transport-layer quotas) (FRU_RSA.1(1))

FRU_RSA.1.1(1) The TSF shall enforce maximum quotas of the following resources: transport-layer representation that a source subject identifier can use over a specified period of time.

5.2.7.3 Maximum quotas (controlled connection-oriented quotas) (FRU_RSA.1(2))

FRU_RSA.1.1(2) The TSF shall enforce administrator-specified maximum quotas of the following resources: controlled connection-oriented resources that users associated with an administrator-specified network identifier and a set of administrator-specified network identifiers can use over an administrator-specified period of time.

5.2.8 TOE Access

5.2.8.1 User-initiated locking (FTA_SSL.2)

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own local interactive session by:

- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the user to re-authenticate prior to unlocking the session.

5.2.8.2 TSF-initiated termination (FTA_SSL.3)*

FTA_SSL.3.1 The TSF shall terminate a **local or** remote session after a Security Administrator-configurable time interval of session inactivity.

5.2.8.3 Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing a user session that requires authentication, the TSF shall display only a Security Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

5.2.8.4 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny establishment of an authorized user session based on location, time, and day.

5.2.9 Trusted Path/Channels

5.2.9.1 Inter-TSF trusted channel (Prevention of disclosure) (FTP_ITC.1(1))

FTP_ITC.1.1(1) The TSF shall use encryption to provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

FTP_ITC.1.2(1) The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for all authentication functions, **[*none*]**.

5.2.9.2 Inter-TSF trusted channel (Detection of modification) (FTP_ITC.1(2))

FTP_ITC.1.1(2) The TSF shall use a cryptographic signature to provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and detection of the modification of data.

FTP_ITC.1.2(2) The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for all authentication functions, **[*none*]**.

5.2.9.3 Trusted path (Prevention of disclosure) (FTP_TRP.1(1))

FTP_TRP.1.1(1) The TSF shall provide an encrypted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

FTP_TRP.1.2(1) The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3(1) The TSF shall require the use of the trusted path for user authentication, all remote administration actions, **[*none*]**.

5.2.9.4 Trusted path (Detection of modification) (FTP_TRP.1(2))

FTP_TRP.1.1(2) The TSF shall use a cryptographic signature to provide a communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and detection of the modification of data.

FTP_TRP.1.2(2) The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3(2) The TSF shall require the use of the trusted path for user authentication, all remote administration actions, **[*none*]**.

5.3 TOE Security Assurance Requirements

The TOE assurance requirements are reproduced from CC Part 3 and are conformant to the following assurance package EAL4 augmented with ALC_FLR.2, and ATE_DPT.3.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.4: Complete functional specification
	ADV_IMP.1: Implementation of the TSF
	ADV_TDS.3: Basic modular design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.4: Product support, acceptance procedures and automation
	ALC_CMS.4: Problem tracking CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.3: Testing: modular design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3: Focused vulnerability analysis

Table 3: Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

Developer action elements

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.

Content and presentation elements

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.

Evaluator action elements

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

5.3.1.2 Complete functional specification (ADV_FSP.4)

Developer action elements

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall **describe all** actions associated with each TSFI.

ADV_FSP.4.5C **The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.**

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Implementation representation of the TSF (ADV_IMP.1)

Developer action elements

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

5.3.1.4 Semiformal modular design (ADV_TDS.3)

Developer action elements

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C **The design shall describe the TSF in terms of modules**.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall **provide a description** of **each subsystem of** the **TSF.**.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C **The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF**.

ADV_TDS.3.7C The design shall describe each **SFR-enforcing module in terms** of **its purpose and relationship with other modules.**

ADV_TDS.3.8C **The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.**

ADV_TDS.3.9C The design shall describe each **SFR-supporting or SFR-non-interfering module in terms** of **its purpose and interaction with other modules.**

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements

ADV_TDS.3.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator ***shall determine*** that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

Developer action elements

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

Content and presentation elements

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 use 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, 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.

Evaluator action elements

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

5.3.2.2 Preparative procedures (AGD_PRE.1)

Developer action elements

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

Content and presentation elements

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 the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle Support (ALC)

5.3.3.1 Production support, acceptance procedures and automation (ALC_CMC.4)

Developer action elements

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements

ALC_CMC.4.1C The TOE shall be labeled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Problem tracking CM coverage (ALC_CMS.4)

Developer action elements

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

Developer action elements

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.

Content and presentation elements

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.

Evaluator action elements

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

5.3.3.4 Identification of security measures (ALC_DVS.1)

Developer action elements

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.3.3.5 Flaw reporting procedures (ALC_FLR.2)

Developer action elements

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.

Content and presentation elements

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 flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation 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.

Evaluator action elements

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

5.3.3.6 Developer defined life-cycle model (ALC_LCD.1)

Developer action elements

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements

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

5.3.3.7 Well-defined development tools (ALC_TAT.1)

Developer action elements

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation elements

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements

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

5.3.4 Tests (ATE)

5.3.4.1 Analysis of coverage (ATE_COV.2)

Developer action elements

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements

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

5.3.4.2 Testing: modular design (ATE_DPT.3)

Developer action elements

ATE_DPT.3.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements

ATE_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

ATE_DPT.3.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.3.3C The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

Evaluator action elements

ATE_DPT.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Functional testing (ATE_FUN.1)

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

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 and describe the scenarios for performing each test. 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.

Evaluator action elements

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

5.3.4.4 Independent testing – sample (ATE_IND.2)

Developer action elements

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

Content and presentation elements

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.

Evaluator action elements

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 a subset of the TSF interfaces to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Focused vulnerability analysis (AVA_VAN.3)

Developer action elements

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E 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 Enhanced-Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions implemented by the TOE to satisfy the SFRs.

6.1 TOE Security Functions

The following security functions are defined for the TOE:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- TSF Protection
- Resource Utilization
- TOE Access
- Trusted Path/Channels.

6.1.1 Security Audit

6.1.1.1 Audit record generation (FAU_GEN.1-NIAP-0410, FAU_GEN.2-NIAP-0410, FPT_STM.1)

The audit trail generated by the TOE comprises several logs, which are stored in the PAN-OS file system:

- Configuration logs—include events such as when an administrator configures the security policies, and when an administrator configures which events gets audited
- System logs—record user login and logout
- Traffic logs—record the traffic flow events
- Threat logs—record the detection and blocking of threats
- Alarm logs – record occurrence and acknowledgement of alarms

Auditing of events captured in the Configuration logs and System logs is always enabled. Auditing of events captured in the Traffic logs can be enabled and disabled via information flow security policies. The setting for traffic logging in a security policy can be viewed in the policy management configuration. Changes to the traffic logging setting are audited in the Configuration log.

The TOE is capable of generating audit records for security-relevant events occurring on the next-generation firewall. 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, and outcome (success or failure) of the event. The TOE provides its own reliable time stamps for use in the audit records. The auditable events are as follow:

- Detection of potential security violation. Audit records include identification of what caused the generation of the alarm. This log will be recorded in the alarm log.
- Acknowledgement of a generated alarm. Audit records include the identity of the administrator that acknowledged the alarm. This log will be recorded in the alarm log.

- Enabling and disabling of any of the analysis mechanisms used to detect potential security violations. Audit records include the identity of the Security Administrator performing the function. This log will be recorded in the configuration log.
- Opening the audit trail. Audit records include the identity of the administrator performing the function. This log will be recorded in the system log.
- Unsuccessful attempts to read information from the audit records. Audit records include the identity of the administrator attempting the function. This log will be recorded in the system log.
- All modifications to the audit configuration that occur while the audit collection functions are operating. Audit records include the identity of the Security Administrator performing the function. This log will be recorded in the configuration log.
- Actions taken due to exceeding the audit threshold. Audit records include the identity of the Security Administrator performing the function. This log will be recorded in the configuration log.
- Actions taken due to audit storage failure. Audit records include the identity of the Security Administrator performing the function. This log will be recorded in the system log.
- Failures of the following cryptographic operations—the audit records include the type of cryptographic operation and any applicable cryptographic modes of operation, but exclude any sensitive information. . These logs will be recorded in the system log.
    - Cryptographic key validation and packing
    - Cryptographic key handling and storage
    - Symmetric key generation
    - Asymmetric key generation
    - Key distribution
    - Key destruction
    - Data encryption/decryption
    - Cryptographic signature services
    - Random number generation
    - Cryptographic hashing
    - Cryptographic key agreement
- Decisions to permit and deny information flows, either between two subjects or between a subject and the TOE (covering all three information flow policies). Audit records include the following information: presumed identity of source subject; identity of destination subject; transport layer protocol, if applicable; source subject service identifier, if applicable; destination subject service identifier, if applicable; identity of the firewall interface associated on which the TOE received the packet; identity of the rule that allowed or disallowed the packet flow, if applicable. This log will be recorded in the traffic log.
- Reaching of the threshold for unsuccessful authentication attempts, the actions taken (e.g., disabling of an account) when the threshold was reached, and (if appropriate) the subsequent restoration to the normal state (e.g., re-enabling of an account). Audit records include the identity of the unsuccessfully authenticated user. This log will be recorded in the system log.
- Successful and unsuccessful use of authentication mechanisms, including all use of the local authentication mechanism. Audit records include the claimed identity of the user attempting to authenticate. This log will be recorded in the system log.
- All use of the user identification mechanism used for authorized users (that is, those that authenticate to the TOE). Audit records include the claimed identity of the user using the identification mechanism. This log will be recorded in the system log.

- Success and failure of binding of user security attributes to a subject. Audit records include identity of the user whose attributes are attempting to be bound. This log will be recorded in the system log.
- All modifications in the behavior of the functions in the TSF. Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- Enabling or disabling of the key generation self-tests. Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- All manipulation of the security attributes. Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes. Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- All modifications of the values of administrator roles and administrative users by the administrator. Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- All modifications of the values of cryptographic security data by the cryptographic administrator. Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- All modifications to the time and date used to form the time stamps by the administrator. Audit records include the identity of the administrator performing the function. This log will be recorded in the system log.
- All modifications to the information flow policy ruleset by the Security Administrator. Audit records include the identity of the Security Administrator performing the function. This log will be recorded in the configuration log.
- All modifications of network interface configurations by the administrator. Audit records include the identity of the Security Administrator performing the function. This log will be recorded in the configuration log.
- All modifications of limits on quotas for transport-layer connections and controlled connection-oriented resources, and actions taken when the quota is exceeded (including the fact that the quota was exceeded). Audit records include the identity of the administrator performing the function. This log will be recorded in the configuration log.
- All attempts to revoke security attributes. Audit records include the list of security attributes that were attempted to be revoked and the identity of the administrator performing the function. This log will be recorded in the configuration log.
- Modifications to the group of users that are part of a role. Audit records include the user IDs that are associated with the modifications and the identity of the administrator performing the function. This log will be recorded in the configuration log.
- Occurrence of a failure or service discontinuity and resumption of regular operation. Audit records include the type of failure or service discontinuity. This log will be recorded in the system log.
- Notification that a replay event occurred. Audit records include the identity of the user that was the subject of the replay attack. This log will be recorded in the threat log.
- Execution of the TSF self tests, including tests for cryptography and key generation components. Audit records include the identity of the administrator performing the test, if initiated by an administrator. This log will be recorded in the system log.
- All TOE capabilities being discontinued due to a failure. Audit records include the TOE capability being discontinued and the type of failure. This log will be recorded in the system log.

- Locking of an interactive session by the session locking mechanism and any attempts at unlocking an interactive session. Audit records include the identity of the user associated with the session being locked or unlocked. This log will be recorded in the system log.
- Termination of a remote session by the session locking mechanism. Audit records include the identity of the user associated with the session being terminated. This log will be recorded in the system log.
- All attempts at establishment of a user session. Audit records include identity of the user attempting to establish the session and, for unsuccessful attempts, the reason for denial of the establishment attempt. This log will be recorded in the system log.
- All attempted uses of the trusted channel functions. Audit records include identification of the initiator and target of all trusted channels. This log will be recorded in the system log.
- All attempted uses of the trusted path functions. Audit records include identification of the claimed user identity. . This log will be recorded in the system log.
- The startup and shutdown of the appliance.

6.1.1.2 Audit review, selection, storage (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1-NIAP-0407, FAU_STG.1)

Through the GUI, the TOE provides the ability to review the audit trail and to search and sort the audit records based on: user identity; source subject identity; destination subject identity; ranges of dates, times, user identities, subject service identities, or transport layer protocol; rule identity; and TOE network interface. All authorized administrators have read access to the audit records. The records are presented in a form suitable for the authorized administrator to interpret the information.

The TOE provides the capability for the Security Administrator to include or exclude auditable events from the set of audited events based on the following criteria: user identity; event type; network identifier; subject service identifier; event success; event failure; rule identity.

The TOE stores the audit records locally and protects them from unauthorized deletion by allowing only users in the Audit Administrator role to access the audit trail with delete privileges. The pre-defined Audit Administrator role defines the privileges permitted for users of this type.

The TOE does not provide an interface where a user can modify the audit records, thus it prevents modification to the audit records.

All logs are stored in the order received. All logs are given a unique sequence number and therefore, sorting can be performed on the sequence number. To view the sequence number, one can export the logs as CSV files from the UI.

The TOE implements the sorting and searching of audit data as follows:

- The audit data is automatically pre-sorted by timestamp. Searching and sorting by timestamp can be performed with a query via the GUI Monitor tab would appear as follows:

  “(receive_time leq '2012/07/23 04:02:04')”

- The audit data can be searched to include a specified range of dates and times.
  - Compound expressions that permit searching with a date and time range are supported with the GUI query builder on the Monitor tab as in: “(receive_time geq '2010/03/01 00:00:00') and (receive_time leq '2010/03/19 00:00:00')”
- The ability to search the audit data by source and destination subject identity - 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 Monitor tab 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.

- The ability to search the audit data by user identity can be performed as follows:
  - For example, a query via the GUI Monitor tab would appear as follows: "(admin eq CCauditadmin)".
- The ability to search the audit data by source and/or destination subject service identifiers can be performed as follows:
  - For example, a query via the GUI Monitor tab would appear as follows: "(port.dst eq 500)".
  - For example, a query for a range via the GUI Monitor tab would appear as follows: "(port.dst geq 200) and (port.dst eq 500)"
- The ability to search the audit data by rule identity can be performed as follows:
  - For example, a query via the GUI Monitor tab would appear as follows: "(rule eq allow_VPN)".
- The ability to search the audit data by the transport layer protocol can be performed as follows:
  - For example, a query via the GUI Monitor tab would appear as follows: "(proto eq udp)"
  - For example, a query for a range via the GUI Monitor tab would appear as follows: "(proto eq udp) or "(proto eq tcp)"
- The ability to search the audit data by the TOE network interfaces can be performed as follows:
  - For example, a query via the GUI Monitor tab would appear as follows: "(interface.src eq 'ethernet1/2')"

It is important to note that the intent of sorting in this requirement is to allow the administrators the capability to organize or group the records associated with a given criteria.

Since the TOE only supports Administrator users, there will not be any unsuccessful attempts to access the audit records thus no audit records will be generated. FAU_SAR.2 is not applicable.

6.1.1.3 Handling of potential audit data loss (FAU_STG.3, FAU_STG.NIAP-0414-1-NIAP-0429)

The Security Administrator is able to set a percentage threshold value for audit storage capacity. If the audit trail exceeds this threshold, the TOE will generate a critical severity event that will result in notification to all administrators currently logged into the system and to the console, whether an administrator is logged in or not. As with FAU_ARP.1, this can be configured to generate an audible alarm and will require acknowledgement from an authorized administrator.

By default, the system will overwrite the oldest logs in the case that the audit trail exceeds the available space. Optionally, a user in the Security Administrator role can set the system to prevent all future auditable events until such time that an Audit Administrator frees up space in the audit trail by deleting existing audit records.

6.1.1.4 Potential violation analysis (FAU_SAA.1-NIAP-0407)

The TOE can apply a set of rules for monitoring events, based on the severity of the event and the type of event (system vs. configuration). The TOE monitors the following events that may indicate a potential security violation:

- Security Administrator specified number of authentication failures
- Security Administrator specified number of Information Flow policy violations by an individual presumed source network identifier (e.g., IP address) within an administrator specified time period

- Security Administrator specified number of Information Flow policy violations to an individual destination network identifier within an administrator specified time period
- Security Administrator specified number of Information Flow policy violations to an individual destination subject service identifier (e.g., TCP port) within an administrator specified time period
- Security Administrator specified Information Flow policy rule, or group of rule violations within an administrator specified time period
- Any detected replay of TSF data or security attributes
- Any failure of the cryptomodule self-tests
- Any failure of the other TSF self-tests
- Security Administrator specified number of encryption/decryption failures

6.1.1.5 Security alarms and acknowledgements (FAU_ARP.1, FAU_ARP_ACK_(EXT).1)

Security Alarms are generated as log messages. For each Security Alarm, the Security Administrator can configure the action that the system will take, including:

- To generate a log
- To forward the log to all management interfaces (i.e. the local console, remote administrator sessions that exist, and remote administrator sessions that are initiated before the alarm has been acknowledged)
- To generate a security alarm (i.e., a log that requires explicit administrator acknowledgement)
- And to generate an audible alarm (i.e., a security alarm that causes a sound to be generated at the destination management interfaces).

For each event where "generate security alarm" is enabled, additional steps will be taken to require acknowledgment of the security alarm and to notify all alarm destinations that acknowledgement was received and by which administrator.

In the evaluated configuration, the events listed in Section 6.1.1.4 will be configured to generate security alarms.

6.1.2 Cryptographic Support

6.1.2.1 Cryptographic module and cryptographic operations (FCS_BCM_(EXT).1, FCS_COP.1(1-5))

The TOE has been FIPS 140-2 validated, with an overall rating of Level 2. Per NIST Cert# 2323 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2323 – Security Policy, the TOE meets FIPS PUB 140-2 level 3 for Roles, Services, and Authentication; Cryptographic Module Specification; and Design Assurance. All other ratings are a minimum of Level 2.

- The TOE incorporates OpenSSL, which provides implementation of the cryptographic algorithms specified in this ST. The FIPS-approved cryptographic functions, which are performed in a FIPS-approved mode of operation, are as follows:Symmetric data encryption and decryption using AES in CBC, ECB or CTR mode, with bit sizes of 128, 192 or 256 bits (algorithm validation certificates #2896 and #2897)
- Cryptographic signature generation and verification using RSA with a key size of 2048 bits (algorithm validation certificate #1525)
- Cryptographic hashing services using SHA-256, SHA-384, or SHA-512 (i.e., Secure Hash Algorithm with message digest sizes of 256, 384 or 512 bits) (algorithm validation certificate #2439)
- Cryptographic hashing services using HMAC-SHA-1, and HMAC-SHA-256 (i.e. Keyed-Hash Message Authentication Code with message digest (algorithm validation certificate #1832).

- Cryptographic key agreement services using Diffie-Hellman (a Finite Field-based key agreement algorithm) with a 2048-bit key size (modulus)
- Cryptographic hashing services using SHA-1 (i.e., Secure Hash Algorithm with message digest size of 160 bits), in support of the TOE's VPN capability (algorithm validation certificate #2439).

6.1.2.2 Cryptographic key generation (FCS_CKM.1(1-2), FCS_COP_EXT.1)

The OpenSSL library included in the TOE employs an ANSI X9.31 compliant random number generator for creation of asymmetric and symmetric keys. It is seeded using a 128-bit seed sourced by the TOE from the kernel's random number generator. This works by gathering entropy from environmental noise via device drivers (disk access, network traffic, etc). The seed source is protected from tampering by virtue of being enclosed within the physical boundary of the TOE appliance, which is assumed to be located in an appropriately physically secure environment.

The TOE generates symmetric cryptographic keys using the FIPS-approved **ANSI X9.31** (algorithm validation certificate #1290) compliant random number generator included in the OpenSSL library. Integrity is assured by error checking within IPSec as well as TCP.

The TOE generates asymmetric cryptographic keys using the RSA algorithm utilizing the FIPS-approved **ANSI X9.31** compliant RNG included in the OpenSSL library. Integrity is assured as follows:

- For keys in storage, the TOE will be a FIPS 140-2 validated cryptographic module, which will provide physical integrity protection in accordance with NIST SP 800-57 "Recommendation for Key Management", Section 6.2.2.2
- For keys in transit, the TOE will use the cryptographic integrity mechanisms provided by HTTPS, consistent with NIST SP 800-57 "Recommendation for Key Management", Section 6.2.1.2.

Available key strengths are equivalent to 128 bit key strength in symmetric keys.

6.1.2.3 Cryptographic key management (FCS_CKM.2, FCS_CKM_(EXT).2, FCS_CKM.4)

The TOE is able to distribute keys using both manual and automated methods. These methods conform with Section 8.1.5 of NIST Special Publication 800-57 "Recommendations for Key Management" and NIST Special Publication 800-56A "Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".

The TOE performs a key error detection check on each internal, intermediate transfer of a key. The TOE stores persistent secret and private keys in encrypted form when not in use. The TOE zeroizes non-persistent cryptographic keys as soon as their associated session has terminated. In addition, the TOE recognizes when a private key expires and promptly zeroizes the key on expiration. The TOE does not permit expired private signature keys to be archived.

The TOE zeroizes all cryptographic keys (secret, private, plaintext, etc.) and all other critical cryptographic security parameters immediately when practical to do so. Private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters stored in intermediate locations for the purposes of transferring the key/critical security parameters (CSPs) to another location are zeroized immediately following the transfer. Zeroization is done by overwriting the storage location with a random pattern, followed by a read-verify. Note that cryptographic keys and CSPs are only ever stored in volatile memory.

6.1.3 Identification and Authentication

6.1.3.1 User attribute definitions (FIA_ATD.1)

The TOE maintains user accounts which it uses to control access to the firewall. When creating a new user account, the administrator specifies a user name (i.e., user identity), a password, and a role. Only one role is specified in the user account per user. The TOE uses the user name and password attributes to identify and authenticate the user when the user logs in via the GUI. It uses the role attribute to specify user permissions and control what the user can do with the GUI.

6.1.3.2 Authentication failure handling (FIA_AFL.1)

The TOE logs all unsuccessful remote authentication attempts in the System Log. The device can be configured to lock a user or authorized IT entity out after a configurable number of unsuccessful authentication attempts. The lock can be configured such that a Security Administrator must manually re-enable the account or it can be configured to last a specified amount of time.

6.1.3.3 Identification and authentication (FIA_UAU.1, FIA_UAU_(EXT).2, FIA_UAU_(EXT).5, FIA_UID.2, FIA_USB.1))

The TOE allows ICMP and SNMP services to access the TOE without authentication. However, for SNMP, the TOE does not support remote configuration (i.e., it is not possible to modify the TOE configuration using unauthenticated SNMP). No other unauthenticated services are able to access the TOE.

The TOE identifies and authenticates all users accessing the TOE functions and data via the GUI. The TOE supports local user authentication using an internal database of user attributes and login credentials, as specified by the Security Administrator. A user attempting to login to the TOE via the GUI is successfully authenticated if the authentication data supplied as part of the login process matches the authentication data associated with the user account in the local database. The user's attributes (as specified in FIA_ATD.1) are associated with the subject acting on behalf of the authorized user following successful authentication.

The TOE authenticates authorized IT entities before allowing them access to TOE functions and data. Authorized IT entities must access the TOE through a VPN tunnel that provides endpoint authentication, data confidentiality, and data integrity.

6.1.4 User Data Protection

6.1.4.1 Concepts

This section introduces a number of concepts that are key to an understanding of the TOE's information flow control capabilities.

Interface Types

The TOE is typically installed between an edge router or other device facing the Internet and a switch or router connecting to the internal network. The physical Ethernet interfaces on the TOE can be configured to support various networking environments, including: Layer 2 switching and VLAN environments; Layer 3 routing environments; and combinations of the two. The basic types of interfaces supported by the TOE are as follows:

- Layer 2—Each Layer 2 interface defined on the TOE must be associated with a VLAN. The same VLAN can be assigned to multiple Layer 2 interfaces, but each interface can belong to only one VLAN. One or more Layer 2 interfaces can be configured for untagged VLAN traffic. The administrator can then define Layer 2 sub-interfaces for traffic with specific VLAN tags
- Layer 3—one or more Layer 3 interfaces can be configured for untagged routed traffic. The administrator can then define Layer 3 sub-interfaces for traffic with specific VLAN tags. Each interface can have multiple IP addresses
- Virtual Wire—a virtual wire binds two Ethernet ports together, which allows the TOE to be installed transparently in the network. A virtual wire accepts all traffic or traffic with selected VLAN tags, but provides no switching, or routing services.

In addition, the TOE supports the following interface types that rely on one of the basic types described above:

- VLAN—for each Ethernet port configured as a Layer 2 interface, the administrator can define a VLAN interface to allow routing of the VLAN traffic to Layer 3 destinations outside the VLAN

- Aggregate Ethernet—two or more Ethernet ports can be combined into a group to increase throughput for a Layer 2 or Layer 3 interface and its sub-interfaces
- Loopback—the administrator can define one or more Layer 3 loopback interfaces, which can be used to manage the firewall, rather than using the management port. Each loopback interface can be associated with a Layer 3 interface (unnumbered) or have their own IP address. A loopback interface for management has not been explicitly excluded but has not been subject to testing in the evaluated configuration.
- High Availability (HA)—each HA interface has a specific function, either configuration synchronizationand heartbeats, or state synchronization.

The TOE guidance documentation identifies an additional interface type that is not included in the evaluated configuration—Tap—which permits connection to a SPAN port for traffic monitoring only (i.e., no firewall functionality).

Security Zones

The TOE groups interfaces into security zones. Each zone identifies one or more interfaces on the TOE. Separate zones must be created for each type of interface (Layer 2, Layer 3, or virtual wire), and each interface must be assigned to a zone before it can process traffic.

Security Policies

Security policies provide the firewall rule sets that specify whether to block or allow network connections, based on the application, the source and destination zones, users, and addresses, and the application service (such as UDP port 67 or TCP port 80). Security policy rules are processed in sequence, applying the first rule that matches the incoming traffic.

Security policies can be defined only between zones of the same type. However, the administrator can create a VLAN interface for one or more VLANs and then apply a security policy between the VLAN interface zone and a Layer 3 interface zone. This has the same effect as applying policies between the Layer 2 and Layer 3 interface zones.

Security policies can also specify security profiles that may be used to protect against viruses, spyware, and other threats after the connection is established.

Security Profiles

Security profiles are configured and applied to firewall policy. Each security policy can specify one or more of the following security profiles:

- 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). Any traffic that matches a firewall policy, which also has an antivirus profile attached causes the traffic flow to be inspected for signature (binary pattern) matching against the installed antivirus signature database. When a match is found, the application protocol of the current session under analysis is used to look up the correct action to take based on the antivirus profile in use.
- Antispyware profiles—determine the combination of methods used to combat spyware—download protection, web site blocking, and detection of traffic from installed spyware. Any traffic that matches a firewall policy, which also has an antispyware profile attached causes the traffic flow to be inspected for signature matching against the installed antispyware signature database. When a match is found, the ID of the matching anti-spyware signature is used to look up the severity of the signature. This severity is then used to find the appropriate action to take based on the configuration of the anti-spyware profile.
- 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). Any traffic that matches a firewall policy, which also has a vulnerability protection profile attached causes the traffic flow to be inspected for signature matching against the installed vulnerability protection database. When a match is found, the ID of the matching vulnerability protection signature is used to look up the severity of the signature. This

severity is then used to find the appropriate action to take based on the configuration of the vulnerability protection profile.

- File blocking profiles—blocks selected file types from being uploaded and/or downloaded, or generate an alert when the specified file types are detected. Any traffic that matches a firewall policy, which also has a file blocking profile attached causes the traffic flow to be inspected to determine the types of files traversing known protocols. The file blocking abilities are not based on file extension – the decoders are looking for specific characteristics (magic numbers) that help to identify what the file type is.
- 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 always generate alerts) and a "white list" of web sites that are always allowed. When an application flow is identified as HTTP, the URL is identified by the protocol decoder, extracted, and used to look up URL category for that URL. The category returned by the URL categorization database is then cross-referenced into the URL Filtering profile to decide what action to take based on the returned URL category. The web site categories are defined by Brightcloud, a 3rd party URL filtering service provider. The efficacy of these web site categories defined by BrightCloud has not been covered in this evaluation.
- Data Filtering profiles—define policies that help prevent sensitive information such as credit card or social security numbers from leaving the network(s) protected by the firewall. Any traffic that matches a firewall policy, which also has a data filtering profile attached causes the traffic flow to be inspected for patterns taken directly from the user are used to match on within Office documents, text files, etc. If a match is found, the corresponding action is taken.

Antivirus, anti-spyware, vulnerability, and file blocking profiles can be combined into Security Profile Groups to simplify management.

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

Other Policies

In addition to Security Policies discussed above, the TOE supports the following types of policy:

- Network Address Translation (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 an internal (trusted) zone to a public (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 matches 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. The SSL policy rules are also applied in sequence to the incoming traffic
- SSH Decryption is checked using the SSH application signature, a policy lookup will occur on the decrypt rule to see if this session should be decrypted.
- Application Override policies—change how the TOE classifies network traffic into applications. For example, if some network applications in the operational environment use non-standard port numbers, the administrator can specify application override rules to ensure that traffic to those ports is classified correctly. As with Security Policies, Application Override policy rules are compared against the incoming traffic in sequence; the first rule that matches the incoming traffic is applied.
- User Identification Agent (UIA) policy enforcement - the UIA provides the firewall with the capability to automatically collect user-specific information, and provides mapping information between IP addresses and network users, that is used in security policy enforcement and reporting. The user id can be an attribute specified in the TOE security policies upon which they are enforced. The UIA works only for IPv4 addresses.

6.1.4.2 Unauthenticated information flow policy (FDP_IFC.1(1), FDP_IFF.1(1))

The TOE enforces the Unauthenticated Information Flow SFP to control the type of information that is allowed to pass through the TOE. The TOE applies security policies and security profiles to network traffic attempting to traverse the TOE to determine what actions to take. The source subjects of the SFP are the physical interfaces on which network packets enter the TOE, while the destination subjects are the physical interfaces to which the network packets are destined, based on addressing information contained in the packets.

The TOE enforces the Unauthenticated Information Flow SFP based on the following subject and information security attributes:

- Source subject security attributes—source security zone to which the physical network interface is assigned
- Destination subject security attributes—destination security zone to which the network interface is assigned
- Information security attributes specifiable in security policies, which provide the information flow rule sets:
    - presumed identity of source subject—source address information within the packet
    - identity of destination subject—destination address information within the packet
    - transport layer protocol (e.g., TCP, UDP)
    - source subject service identifier (e.g., source port number)
    - destination subject service identifier (e.g., destination port number)
    - application
    - user
- Information security attributes for stateful packet inspection—for connection-oriented protocols (e.g., TCP), the sequence number, acknowledgement number, and flags (SYN, ACK, RST, FIN); and for connectionless protocols (e.g., UDP), the source and destination network identifiers; and source and destination service identifiers. Note that the TOE uses an IP-based network stack.

The TOE keeps state about connections or pseudo-connections and uses the information to permit or deny information flow. The TOE permits information flow between two subjects (i.e., from the physical interface on which network traffic entered to the physical interface determined by the destination address in the network packet) only where a security policy is defined between the source and destination zones that includes a rule that grants permission, based on the information security attributes listed above and the corresponding settings in the policy rule.

A security policy rule includes the following attributes against which network packets can be compared:

- Source Zone, Destination Zone—zones must be of the same type (Layer 2, Layer 3, or Virtual Wire). Multiple zones can be specified in a single rule to simplify management
- Source Address, Destination Address—the IPv4 or IPv6 addresses for which the rule applies. Addresses must first be defined by the administrator, who specifies a name for the address and the actual IPv4 or IPv6 addresses to be associated with that name. Addresses can be specified as a single address, an address with a mask, or an address range. Addresses can also be combined into address groups to simplify management
- Source User—the source users or user groups subject to the policy rule. These are established using the User Identification Agent
- Application—specific applications covered by the rule. The TOE identifies several categories of applications, including: business-system applications (e.g., auth-service, databases, office program, software updates); collaboration applications (e.g., email, instant messaging, voip-video, social networking, web posting); general internet applications (e.g., file sharing, internet utility); media applications (e.g., audio streaming, gaming, photo video); networking applications (e.g., encrypted-tunnel, ip-protocol, proxy, remote-access, routing); and unknown applications
- Service—specifies services to limit applications to specific protocols and port numbers.

A security policy rule also includes the following attributes that determine what the TOE does with the network packet:

- Action—can be 'allow' or 'deny'
- Profiles—specifies any checking to be performed by the security profiles described above (i.e., antivirus, anti-spyware, vulnerability protection, data filtering, file blocking)
- Options—specifies the following additional processing options for network packets matching the rule:
    - Log Setting—generate log entries in the local traffic log
    - Schedule—limits the days and times when the rule is in effect (e.g., an 'allow' rule might be active only during normal business hours)
    - QoS Marking—change the Quality of Service (QoS) marking on packets matching the rule
    - Disable Server Response Inspection—disables packet inspection from the server to the client, which may be useful under heavy server load conditions.

Prior to matching packets with the policy rules, fragmented packets are reassembled. Upon receiving a packet that is not associated with an established session (a packet with the SYN flag set without a corresponding ACK flag being set), the packet will be matched to the security rules to make a determination of whether to allow or deny the information flow. If the packet is associated with an established session (packet sequence number, acknowledgment number, and flags match an existing session record), the information flow is permitted.

The information flow configuration screen provides the Security Administrator with a way to see which information flows are permitted and which are disabled. It can be viewed before enabling that policy on the device.

The TOE rejects requests for access or services when received on an interface that is not associated with the source address from which the information flow is sourced. Access or service requests are also rejected when the presumed source identity specifies a broadcast identity or a loopback identifier. In addition, requests in which the information received contains the set of host network identifiers by which information is to travel from the source subject to the destination subject are rejected.

Following is a more detailed description of the TOE's firewall capability.

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 (such as applicable NAT, SSL or SSH policies or security profiles). If it is a new connection, the TOE retrieves the source and destination zones and performs an initial policy lookup. If a policy is defined for the zone pair (i.e., source and destination zones) a session is created and packet processing 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. Some applications, such as http, may just be a tunnel for additional applications. To address this scenario the data may be passed through these steps more then once. If the initially detected application is one that has additional applications defined that use it as a transport it will be parsed again. This allows the system to correctly identify a web based IM client as a messaging application rather then as basic http web browsing. It is in this step that the URL is captured and categorized for use later by the URL filtering capability.
- 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)
    - The source user (when available)

- If a security policy is found, the policy rules are compared against the incoming traffic in sequence and the first rule that matches the traffic is applied. If a NAT policy or an SSL or an SSH policy is found, the policy rules are also compared against the incoming traffic in sequence. If a policy rule matching all of the traffic attributes listed above is not found, or if it is found and it specifies a deny action, then the packet is dropped and the session is deleted
- If the application flow is allowed and no further security profiles are applied then it is forwarded. If the session had previously been SSL or SSH 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 signature processor.

6.1.4.3 Unauthenticated TOE services policy (FDP_IFC.1(2), FDP_IFF.1(2))

Any traffic that matches a firewall policy, which also has a security profile attached causes the traffic flow to be inspected for signature matching against the installed security profile signature database. When traffic is sent to the TOE, the set of unified stream based signatures, instantiated from the installed security profile signature database, is applied to the flow. Unified stream based signatures allow the firewall to match packet data against our full set of threat prevention signatures in a single pass. Antivirus, anti-spyware, and intrusion prevention signatures are all compared against the data simultaneously. 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.

The TOE enforces the unauthenticated TOE services SFP based on the following subject and information security attributes:

- Source subject security attributes – source security zone and/or presumed source address
- TOE's network identifier
- Information security attributes – presumed identity of source subject, identity of destination subject, transport layer protocol, source subject service identifier, destination subject service identifier, ICMP message type and code (as specified in RFC 792).

The device permits information flow between a source subject and the TOE when the information security attributes match an information flow control policy specified by the Security Administrator. The device provides a setting such that the Security Administrator can enable or disable ICMP and SNMP for all users. The information flow configuration screen provides the Security Administrator with a way to see which information flows are permitted and which are disabled. It can be viewed before enabling that policy on the device. The device rejects requests for access or services when received on an interface that is not associated with the source address from which the information flow is sourced. Access or service requests are also rejected when the presumed source identity specifies a broadcast identity or a loopback identifier. Additionally, requests in which the information received contains the set of host network identifiers by which information is to travel from the source subject to the destination subject are rejected.

6.1.4.4 VPN policy (FDP_IFC.1(3), FDP_IFF.1(3), FPT_ITC.1)

The TOE supports Virtual Private Networks (VPNs), which allow systems to connect securely over a public wide area network (WAN) as if they were connecting over a local area network (LAN). The TOE uses the IP Security (IPSec) set of protocols to set up a secure tunnel for the VPN traffic, and the private information in the TCP/IP packets is encrypted when sent through the IPSec tunnel.

The TOE uses the Internet Key Exchange (IKE) protocols to automatically generate security keys for communication through the tunnels.

The TOE can be configured for *route-based* VPNs, which allow the TOE to connect to other Palo Alto Networks firewalls (peer TOEs) at central and remote sites. While the TOE can also connect with third party security devices at other locations, this has not been subject to testing in the evaluated configuration and is not covered by this evaluation. With route-based VPNs, the firewall makes a routing decision based on the destination IP address. If traffic is routed through a VPN tunnel, then it is encrypted as VPN traffic. It is not necessary to define special rules

or to make explicit reference to a VPN tunnel; routing and encryption decisions are determined only by the destination IP address.

For the IPSec connection between the firewalls, the full IP packet (header and payload) is embedded in another IP payload, and a new header is applied. The new header uses the IP address of the outgoing firewall interface as the source IP address and the incoming firewall interface at the far end of the tunnel as the destination IP address. When the packet reaches the firewall at the far end of the tunnel, the original packet is reconstructed and sent to the actual destination host.

IPSec Security Associations (SAs) are defined at each end of the IPSec tunnel to apply all of the parameters that are required for secure transmission, including the security parameter index (SPI), security protocol, cryptographic keys, and the destination IP address.

IKE provides a standard mechanism for generating and maintaining security keys for identification and authentication of traffic through IPSec tunnels:

- Identification—The identification process involves recognition of the peers at both ends of the IPSec tunnel. Each peer is identified by IP address or peer ID (contained in the payload of the IP packet). The firewall or other security device at each end of the tunnel adds the identification of the peer at the other end into its local configuration.
- Authentication—The TOE uses pre-shared keys for authentication.

The TOE supports definition of IKE gateways, which specify the configuration information necessary to perform IKE protocol negotiation with peer gateways.

The Security Administrator can define IPSec and IKE crypto profiles that determine the protocols and algorithms used to negotiate the IPSec and IKE SAs. Crypto profiles are related to standard proposal fields in IKE negotiation. The IKE-crypto profile corresponds to IKE SA negotiation (IKEv1 Phase-1), while the IPSec crypto profile corresponds to IPSec SA negotiation (IKEv1 Phase-2).

The TOE provides the following options for IKE SAs:

- Diffie-Hellman (DH) Group—Select DH group (only DH group 14 is supported in CC mode) to use when generating public keys for IKE, using Diffie-Hellman key agreement
- Encryption—Select encryption algorithms. The TOE supports AES with bit sizes of 128, 192 or 256 bits
- Hash Algorithm—Select hash algorithms. The TOE supports SHA-1
- Lifetime—Specify the length of time that the negotiated key will stay effective.

The TOE provides the following options for IPSec SA:

- Authentication Header (AH)—Select options for authentication and data integrity. The TOE supports SHA-256, SHA-384, or SHA-512
- Encapsulating Security Payload (ESP)—Select options for authentication (SHA-1) and encryption (AES with bit sizes of 128, 192 or 256 bits)
- Perfect Forward Security (PFS) Diffie-Hellman (DH) group—Select DH groups to use in generating independent keys for IPSec. Only DH group 14 is supported in CC mode.
- Lifetime—Specify the length of time that the negotiated key will stay effective.

6.1.4.5 Residual information protection (FDP_RIP.2)

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 by overwriting unused parts of the buffer with 0s.

6.1.4.6 TLS Processing

The TOE uses the OpenSSL program for cryptographic support. The TOE uses TLS v1.0 to decrypt TLS 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. Cryptographic keys are generated on the dataplane and destroyed when the session is destroyed. Key generation is automatic, and key destruction in the TOE is to free-up the memory and then overwriting it the next time that memory is needed by a process. TLS v1.0 is also used in the TOE to protect the integrity of communication between the User Identification Agent and the firewall (see also Section 6.1.6).

The supported cipher suites are:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

6.1.5 Security Management

The TOE provides a GUI management interface to support security management of the TOE. The GUI is accessible via direct connection to the management port on the device, or remotely over HTTPS. The management interfaces enable the authorized administrators to configure the TOE functions and to manipulate TOE data.

6.1.5.1 Security management roles (FMT_SMR.2)

By default, the TOE has the following pre-defined custom administrator roles: auditadmin, cryptoadmin, and securityadmin. These administrator roles were created where there is no overlap in capabilities, except that all have read-only access to the audit trail (except audit administrator with full read/delete access). All roles can administer the TOE both locally and remotely.

The guidance documentation for the evaluated version of the TOE indicates the Superuser role is intended only for initial configuration, to create the administrator accounts for the Security Administrator, Audit Administrator, and Cryptographic Administrator, and that during normal operation the Superuser, Superuser (read-only), Device Administrator, Device Administrator (read-only), Virtual System Administrator, and Virtual System Administrator (read-only) admin roles are not to be assigned to administrators.

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

6.1.5.2 Security management functions

The security management functions provided by the TOE and the roles to which they are restricted are listed in the following table.

Function	Role	Relevant SFRs
Delete audit records	Audit Administrator	FAU_STG.1
Manage audit storage capacity	Security Administrator	FAU_STG.3
Manage prevention of audit loss	Security Administrator	FAU_STG.NIAP-0414-1.1-NIAP-0429
Define and view information flow policy rule set	Security Administrator	FDP_IFF.1(1)
View information flows allowed by policy	Security Administrator	FDP_IFF.1(2)

Function	Role	Relevant SFRs
Manage authentication failure handling	Security Administrator	FIA_AFL.1
Modify behavior of TSF Self Test. The TOE does not implement non-cryptographic self-tests. All self-tests are cryptographic in nature.	Security Administrator	FMT_MOF.1(1)
Enable and disable cryptographic test functions: the cryptographic self-tests can be manually executed at any time by an authorized Cryptographic Administrator. Disabling the cryptographic self-tests would violate the requirements of FIPS140-2 and is therefore not permitted in Common Criteria mode. Software integrity self-tests are considered a different class of cryptographic self-test since they utilize cryptographic algorithms and key material.	Cryptographic Administrator	FMT_MOF.1(2)
Manage security audit review	All administrators	FMT_MOF.1(3)
Manage potential violation analysis parameters (e.g., number of authentication failures, number of information flow policy violations, number of encryption or decryption failures). Manage the set of audited events.	Security Administrator	FMT_MOF.1(4)
Manage security alarms	Security Administrator	FMT_MOF.1(5)
Manage unauthenticated TOE services: Enabling or disabling ICMP or SNMP responses from the management interface of the device to unauthenticated users is controllable by the Security Administrator. ICMP and SNMP are the only services for which the management interface will respond to an unauthenticated user. The Security Administrator can specify whether these services are on or off and if on, the source IP addresses that they will respond to.	Security Administrator	FMT_MOF.1(6)
Manage controlled connection-oriented resources: Only the Security Administrator role is able to configure the connection-oriented resource allocations. The Security Administrator is able to set this per security zone, where security zone can represent a network identifier or set of network identifiers. In addition, the Security Administrator can specify the period of time over which the quota is allocated (by default, this is set to 1 second).	Security Administrator	FMT_MOF.1(7)
Manage SFP attributes: Only a Security Administrator is able to specify what unauthenticated TOE services are available and the policy definitions to enforce service availability, or to configure VPNs	Security Administrator	FMT_MSA.1
By default, the device provides a restrictive information flow policy ruleset - specifically, it does not allow any traffic through the device. There are no options to change this default behavior. By default, only the out of band management interface will respond to traffic initiated to the TOE, and the only services it will listen to are HTTPS, ICMP, and SNMP. HTTP, Telnet, and Panorama are all off by default. For all other interfaces, the default is to have all management off until an authorized administrator turns them on. Specify alternative initial values of security attributes	Security Administrator	FMT_MSA.3-NIAP-0409 (1)(2) FMT_MSA.3

Function	Role	Relevant SFRs
Manage administrator roles and administrative users	Security Administrator	FMT_MTD.1(1)
Modify cryptographic security data	Cryptographic Administrator	FMT_MTD.1(2)
Set date and time	Security Administrator	FMT_MTD.1(3)
Manage information flow policy rules	Security Administrator	FMT_MTD.1(4)
Manage interface configuration	Security Administrator	FMT_MTD.1(5)
Manage transport layer quotas	Security Administrator	FMT_MTD.2(1)
Manage connection-oriented quotas	Security Administrator	FMT_MTD.2(2)
Revoke security attributes For immediate revocation of a user, the TOE is in High Availability (HA) mode and system reboot is required after the user is deleted. Since the TOE is in HA configuration, no data sessions will be affected and any other users in session will simply have to login again.	Security Administrator	FMT_REV.1
Manage session locking timeout	Security Administrator	FTA_SSL.2
Manage session termination timeout	Security Administrator	FTA_SSL.3
Manage TOE access banner	Security Administrator	FTA_TAB.1

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 review the audit trail.

6.1.6 TSF Protection

6.1.6.1 Inter-TSF confidentiality during transmission (FPT_ITC)

The TOE provides the ability to create an IPSec tunnel between the TOE and external VPN Peers. The communications between the TOE and VPN Peers are protected from disclosure by the encryption capabilities of IPSec (the AES algorithm with 128, 192, or 256 bit key sizes).

6.1.6.2 Fault-tolerant operation (FRU_FLT.1, FPT_FLS.1)

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.

6.1.6.3 Manual recovery (FPT_RCV.1)

If there is a failure or service discontinuity of the device, there are generally three types of responses that the device will automatically take. First, if there is simply a process failure, the process will often be restarted. When this happens, the secure state of the device is protected. For example, if the management server fails and has to be restarted, all management connections must be re-authenticated. Second, if the failure causes the device to restart, then the device will restart. When this happens, a local administrator can put the device into maintenance mode or can let the device reboot. If the device reboots, it is in a secure state, with all connections requiring re-checks on the policy and all administrators being re-authenticated. Third, if failure is cryptographic in nature, or occurs during self-testing, the firewall will immediately shut down and enter maintenance mode. In maintenance mode, the ability to return the TOE to a secure state is provided.1

6.1.6.4 Replay detection (FPT_RPL.1)

The device will detect replay attacks against an administrator's session, log the event as an audit/security event, and will reject the data. This is true only for traffic destined for the TOE itself.

6.1.6.5 Self testing (FPT_TST_(EXT).1, FPT_TST.1(1), FPT_TST.1(2))

The TOE meets FIPS 140-2 requirements and therefore provides self-tests at start-up (which are also on-demand tests available to administrators) on all cryptographic functions. Conditional self-tests are also run during the course of normal operation. Methods are provided to verify the integrity of stored TSF executable code and TSF data. Software integrity tests are considered cryptographic in nature because they make use of cryptographic algorithms and cryptographic keying material in their execution.

The device executes self-tests during startup, on demand, and periodically to demonstrate the correct operation of: key error detection, cryptographic algorithms, and RNG. The TSF provides methods to verify TSF data and TSF executable code related to cryptography using cryptographic functions.

The devices executes self-tests following key generation to demonstrate correct operation. Failed self-tests comply with FIPS 140-2 requirements, i.e., a generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited. If a self-test fails, the TOE enters an error state and outputs an error indicator. The TOE doesn't perform any cryptographic operations while in the error state. All data output from the TOE is inhibited when an error state exists. Executable code and data related to key generation used by the TSF-provided cryptographic functions can be verified by the cryptographic administrator.

6.1.6.6 Internal TOE TSF data transfer (FPT_ITT.1)

The TOE uses the OpenSSL program for cryptographic support. TLS is used 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 automatically collect user information. Firewall communications across HA1 (control link) are protected using an SSHv2-secured channel. This secure channel utilizes RSA-2048 for endpoint authentication, AES-256 for confidentiality, and SHA-1 HMAC for message authentication. The TOE uses an **ANSI X9.31** compliant random number generator implemented in PAN-OS for key generation and uses a FIPS-approved method for key destruction. Cryptographic keys are generated on the dataplane and destroyed when the session ends.

6.1.7 Resource Utilization

6.1.7.1 Maximum quotas (FRU_RSA.1(1), FRU_RSA.1(2))

The device is able to enforce transport-layer quotas for the following:

- TCP SYN per second: the number of SYN requests per second
- UDP connections per second: the number of UDP packets per second that do not match an existing UDP session
- ICMP packets per second: the number of ICMP packets per second.

All of the above are configured on what the device calls a "zone protection profile." The zone protection profile is applied to a set of security zones on the firewall where protection is needed. A security zone represents one or more networking interfaces and therefore represents one or more network subnets or network entities. For each of the above and for each security zone, the administrator is able to specify the rate where an audit record is created and the rate where a blocking action is taken. Blocking in the case of the SYN quota being exceeded is performed by implementing random early drop algorithm. Alternatively, SYN cookies may be used to validate a connection before a TCP session is allocated in the firewall's session table.. Blocking in the case of UDP or ICMP is performed by the device dropping all additional packets for the remainder of the second. So, for example, if the UDP threshold is set to 10,000 new UDP sessions/packets per second, and that is hit in the first 100 milliseconds, then all UDP packets will be dropped for the remainder of the second that do not match an existing UDP session.

The TOE also includes a DoS (Denial of Service) Protection rulebase that extends the capabilities listed above. The rulebase allows the specification of a maximum rate of SYN packets, UDP packets, ICMP packets, ICMPv6 packets, and other IP packets based on an individual source IP address, destination IP address, or a combination of the two. The DoS Protection rulebase also allows for the specification of a maximum number of sessions (transport-layer and connection-oriented resources) associated with a particular source IP, destination IP, or source IP and destination IP pair.

The Resource utilization function is designed to satisfy the following security functional requirements:

- FRU_RSA.1(1): The TSF represents a transport-layer communication pathway as a connection. The TOE can defend itself and the resources it protects from various DoS and DDoS attacks by rate limiting these connections (i.e., applying a maximum quota to the number of connections). TCP SYN flood attack protection is one of them.

- FRU_RSA.1(2): The TSF utilizes a session table to control connection oriented resources. The TSF supports both source based session limiting and destination based session limiting to prevent session table flooding attacks. The thresholds for the same are configurable by the security administrator. Also, the Security Administrator has the ability to define the maximum number of resources a particular address or set of addresses can use over a specified time period.

6.1.8 TOE Access

6.1.8.1 Session management (FTA_SSL.2, FTA_SSL.3, FTA_TAB.1, FTA_TSE.1)

At any time, the user can log out of their current local session without losing the context in which they were working. Upon re-authenticating, the user can resume where they left off in the previous session. After logging out, all device access is disabled.

The TOE provides the Security Administrator with a configurable timeout after which local and remote sessions are logged out. After the timeout elapses, all device activity is disabled and the user may not access device contents.

Remote sessions established through HTTPS (web interface) can be configured by the Security Administrator to timeout after a specified period of time.

The TOE provides the Security Administrator the capability to create a custom advisory notice or consent warning message to be displayed prior to establishing a user session.

The TOE provides the Security Administrator the ability to control when (e.g., time and day) and where (e.g., from a specific network address) remote administrators, as and authorized IT entities can access the TOE. The security administrator can restrict the establishment of an administrative session based on a schedule (i.e., day and time) and based upon the originating source IP address (or subnet).

6.1.9 Trusted Path/Channels

6.1.9.1 Inter-TSF trusted channels (FTP_ITC.1(1), FTP_ITC.1(2))

The TOE provides virtual private networking (VPN) connectivity to remote devices using IKE/IPSec. Such communications provide for the prevention of disclosure by using encryption on all data that is passed between the two VPN endpoints. IKE/IPSec tunnels built to an authorized IT entity utilize the AES algorithm (128-, 192-, or 256-bit key sizes). IKE/IPSec also provide for the detection of modification of data passed through the VPN tunnel. The modification of data is detected by computing a signature (using an industry-standard SHA-1 HMAC algorithm) on all data transmitted through the tunnel.

The TOE does not make use of NTP (to provide system time updates) or certificate authority servers (to authenticate administrators). The TOE includes all required management functionality and does not rely on authorized IT entities for configuration or management.

6.1.9.2 Trusted path (FTP_TRP.1(1), FTP_TRP.1(2))

Remote users can initiate communication with the TOE via the trusted path using HTTPS encrypted data streams. Administration sessions are authenticated with the digital signature algorithm specified in FCS_COP.1(2). All remote administration actions and user authentication take place in these secured channels. Authentication with a digital signature algorithm works by hashing the data to be transmitted, and then encrypting that hash with the RSA private key. When the communication peer receives the data and the digital signature, it decrypts the encrypted hash with the RSA public key, and then compares that with its own hash of the data that was transferred. If both hashes match, then the authenticity and integrity of the data are guaranteed.

HTTPS data encryption and decryption is performed using AES algorithm operating in CBC mode with cryptographic key size of 128 and 256 bits.

HTTPS communication utilizes a SHA-1 based Keyed Message Authentication Code (HMAC) to detect the modification of data. The modification of data is detected by computing a hash of the data appended by a secret key known only to the two endpoints of the secure channel. If an intermediate party intercepts the message and modifies the data, the receiving endpoint will detect the modification by computing the HMAC using the secret key and will identify that the signature transmitted with the message does not match the data. The affected message will be discarded by the TOE. This path is used in all user authentication and remote administration actions.

7. Protection Profile Claims

As documented in this Security Target (ST), the TOE (Palo Alto Networks Next-Generation Firewalls) meets all of the Security Functional Requirements (SFRs) from the following Protection Profile (PP): the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, July 25, 2007.

The Security Problem Definition and Security Objectives in this ST have been reproduced from the PP with the exceptions noted at the end of this section.

The ST has not included FTA_SSL.1, which is specified in the PP. The TOE does not support TSF-initiated session locking. Instead, the TOE terminates all sessions after a configurable period of inactivity. FTA_SSL.3 has been refined to specify this behavior (see below). The ST specifies stricter requirements than the PP, and so satisfies the PP requirement of demonstrable conformance.

The ST has refined some SFRs reproduced from the PP, as follows:

- FAU_GEN.1.1-NIAP-0410, item b): "3" is replaced with "2" to provide an accurate reference to the table of auditable events consistent with the ST's table numbering
- FAU_GEN.1.2-NIAP-0410, item b): "3" is replaced with "2" to provide an accurate reference to the table of auditable events consistent with the ST's table numbering
- Table 2: Auditable Events, FAU_ARP_ACK_(EXT).1: The ST replaces "None" with "Acknowledgement of alarm". It is clear the PP intended an auditable event for this SFR, since it specifies additional audit record contents for the SFR
- Table 2: Auditable Events, FCS_COP.1(4): The ST adds additional audit record contents for this SFR, where the PP does not specify any. This makes the specification of audit data for FCS_COP.1(4) consistent with the other iterations of FCS_COP.1 specified in the PP and ST
- Table 2: Auditable Events, FMT_MTD.1(1): Refined to identify the specific TSF data covered by FMT_MTD.1(1), consistent with the refinement made to FMT_MTD.1(1) (see below)
- Table 2: Auditable Events,FMT_MTD.2(1), FMT_MTD.2(2): minor refinements to make the descriptions of auditable events for these SFRs grammatically correct
- Table 2: Auditable Events: added appropriate entries for FDP_IFC.1(3), FDP_IFF.1(3), FMT_MSA.3, FPT_FLS.1, FPT_ITT.1, and FRU_FLT.1, which are additional SFRs not specified in the PP
- FCS_CKM_(EXT).2.3: refined to specify that non-persistent cryptographic keys are destroyed as soon as their associated sessions end, rather than allowing the administrator to specify the period of time before zeroization. This is a stricter requirement than that specified in the PP, and so satisfies the PP requirement of demonstrable conformance
- FCS_CKM_EXT.1: not included in the ST because, while it is listed in the table of auditable events in the PP, it does not exist elsewhere in the PP. It appears that this was a typo in the PP
- FDP_IFF.1.2(1), second bullet point: removed "source" and added "subject", changing the SFR from "set of source destination identifiers" to "set of destination subject identifiers", which specifies the intent of the PP
- FMT_MSA.1.1: refined to include the VPN SFP within the scope of the SFR and to provide correct spelling of "policies", which is misspelled as "polices" in the PP
- FMT_MOF.1(2): refined to exclude the ability to disable TSF cryptographic self-tests. Cryptographic self-tests are required in order to maintain FIPS 140-2 compliance.
- FMT_MTD.1.1(1), FMT_MTD.1.1(5): refined to specify the specific TSF data and specific administrative role, consistent with the intention of the PP as expressed in the PP application note

- FMT_MTD.1(3): refined to exclude the ability for authorized IT entities from altering the system time and date used to form time stamps
- FTA_SSL.3: refined to specify local or remote sessions are terminated after a time interval of session inactivity.
- FAU_SAA.1: refined to specify a single admin-specified threshold for encryption and decryption failures rather than one threshold for encryption failures and another for decryption failures.

The PP includes two identical statements of FIA_UAU.1. Only one of these is identified as an iteration. The ST author has therefore determined that only one statement of FIA_UAU.1 is required in the ST.

The PP also specifies SFRs for the IT environment. Version 3.1 of the Common Criteria does not require that requirements on the IT (operational) environment be specified as SFRs. Therefore, these SFRs have not been reproduced in the ST.

The following requirements are added to the ST:

- FDP_IFC.1(3) and FDP_IFF.1(3) are added to specify the VPN capabilities of the TOE
- FCS_COP.1(5) is added to specify use of SHA-1, in support of the TOE's VPN capability. The TOE requires the use of SHA-1 for message authentication within IKE and IPSec. The reason is backward compatibility with IPSEC. The TOE implements IPSEC so this is a valid rationale for the use of SHA-1. SHA-1 is FIPS-approved for HMAC (keyed message authentication) applications like this one
- FPT_ITC.1 is added to support the VPN capability by specifying the confidentiality of TSF data when transmitted to another trusted IT product over the VPN
- FMT_MSA.3 is added to specify requirements for static attribute initialization within the scope of the VPN SFP
- 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 rationale for these SFRs addressing security objectives specified in the PP is presented in Section 8.2.

All assumptions and objectives from the PP have been included except for the following:

- 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.
- O.DOCUMENT_KEY_LEAKAGE is removed because this is mapped to the AVA_CCA_(EXT).2 assurance requirement which is not claimed in this ST.
- O. SOUND_DESIGN is removed because this is mapped to the ADV_INT.1, ADV_FSP.5 and ADV_TDS.4 all of which are not claimed in this ST.

The ST adds the following security objectives for the operational environment to address the assumptions added by the ST: OE.UIA_ONLY.

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
- Requirement Dependencies
- PP Claims.

8.1 Security Objectives Rationale

Sections 6.1 and 6.2 of the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments provides rationale for the security objectives, demonstrating the PP security objectives are suitable to address the security problem definition described in the PP. The rationale is valid for the PP objectives reproduced in this and is not further discussed. Exceptions to the Security Problem Definition and the set of security objectives specified in the PP are noted in Section 7..

8.2 Security Functional Requirements Rationale

Section 6.3 the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments provides 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. These additional security functional requirements contribute to addressing security objectives specified in the PP, as follows:

- FDP_IFC.1(3) and FDP_IFF.1(3) ensure the TOE mediates traffic over configured VPNs. As such, these components trace back to and contribute to meeting O.MEDIATE
- FCS_COP.1(5) ensures the TOE provides SHA-1 cryptographic hashes that support the TOE's ability to mediate traffic over configured VPNs. As such, this component traces back to and contributes to meeting O.MEDIATE
- FPT_ITC.1 specifies requirements for the confidentiality of TSF data when transmitted to another trusted IT product, which supports the VPN capability specified by FDP_IFC.1(3) and FDP_IFF.1(3), by ensuring secure establishment of the VPN tunnel. As such, this component also traces to O.MEDIATE
- FMT_MSA.3 specifies requirements for and restrictions on the management of security attributes associated with the VPN SFP. As such, it traces back to and aids in meeting O.MANAGE
- FRU_FLT.1 and FPT_FLS.1 ensure that the TOE continues to perform information flow control in case of failure. These components trace back to and aid in meeting the O.MAINT_MODE security objective, by providing a mode in which recovery of the TSF can be performed.
- FPT_ITT.1 ensures that communication of TSF data between separate TOE components is protected. This component traces back to and aids in meeting the O.SELF_PROTECTION security objective, by ensuring protection of TSF data from detection or tampering when it is communicated between separate parts of the TOE (i.e., the firewall appliance and the User Identification Agent).

The ST includes security functional requirements that match those in the PP. In some cases, the security functional requirements are not applicable to the TOE as follows:

- FMT_SMR.2.3 ensures that all administrators can invoke the self-tests. The TOE utilizes cryptographic mechanisms in all self-tests so the permissions are restricted to the cryptographic administrator. The PP further specifies that administrators other than the cryptographic administrator are not authorized to perform cryptographic initialization and management functions.

8.3 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL4 augmented with ALC_FLR.2 and ATE_DPT.3. This target was chosen to ensure that the TOE has a moderate to high level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to provide the added assurances from having flaw remediation procedures and test coverage analysis that demonstrates depth of coverage of the test suite.

8.4 Requirement Dependency Rationale

Section 6.5 of the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments provides the requirement dependency analysis for the security functional requirements specified in the PP. The rationale in the PP is valid for this ST as the ST reproduces all PP requirements. The following table therefore analyzes the dependencies only of the requirements that have been added to this ST.

Requirement	Dependencies	Included
FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	**See rationale**
FDP_IFC.1(3)	FDP_IFF.1	Yes [FDP_IFF.1(3)]
FDP_IFF.1(3)	FDP_IFC.1, FMT_MSA.3	Yes [FDP_IFC.1(3)]
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes
FRU_FLT.1	FPT_FLS.1	Yes
FPT_FLS.1	None	Not applicable
FPT_ITC.1	None	Not applicable
FPT_ITT.1	None	Not applicable

Table 4: Requirement Dependency Summary

The dependencies of FCS_COP.1(5) on [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] and FCS_CKM.4 are not applicable, because FCS_COP.1(5) specifies requirements for a cryptographic hash mechanism (SHA-1), which does not require keys to be either generated, imported, or destroyed.

8.5 PP Claims Rationale

See Section 7, Protection Profile Claims.

A. Statistical Random Number Generator Tests

Note: These tests are reproduced from Appendix A of the U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, Version 1.1, July 25, 2007.

A cryptographic module employing random number generators (RNGs) shall perform the following statistical tests for randomness. A single bit stream of 20,000 consecutive bits of output from each RNG shall be subjected to the following four tests: monobit test, poker test, runs test, and long runs test. (These four tests are simply those that formerly existed as the statistical RNG tests in Federal Information Processing Standard 140-2. However, for purposes of meeting this protection profile, these tests must be performed at the frequency specified earlier in this protection profile.)

The Monobit Test:

1. Count the number of ones in the 20,000 bit stream. Denote this quantity by X.
2. The test is passed if 9,725 < X < 10,275.

The Poker Test:

1. Divide the 20,000 bit stream into 5,000 contiguous 4 bit segments. Count and store the number of occurrences of the 16 possible 4 bit values. Denote f(i) as the number of each 4 bit value i, where 0 < i < 15.
2. Evaluate the following:

$$X = (16 / 5000) * \left(\sum_{i=0} [f(i)]^2 \right) - 5000$$

3. The test is passed if 2.16 < X < 46.17.

The Runs Test:

1. A run is defined as a maximal sequence of consecutive bits of either all ones or all zeros that is part of the 20,000 bit sample stream. The incidences of runs (for both consecutive zeros and consecutive ones) of all lengths (> 1) in the sample stream should be counted and stored.
2. The test is passed if the runs that occur (of lengths 1 through 6) are each within the corresponding interval specified in the table below. This must hold for both the zeros and ones (i.e., all 12 counts must lie in the specified interval). For the purposes of this test, runs of greater than 6 are considered to be of length 6.

Length of Run	Required Interval
1	2343 – 2657
2	1135 – 1365
3	542 – 708
4	251 – 373
5	111 – 201
6 and greater	111 – 201

Table C.1 - Required Intervals for Length of Runs Test

The Long Runs Test:

1. A long run is defined to be a run of length 26 or more (of either zeros or ones).
2. On the sample of 20,000 bits, the test is passed if there are no long runs.