Security Target

Juniper Networks Secure Access Family Version 6.4

Document Version 1.9

February 26, 2010

Prepared For:

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net

Prepared By:

Apex Assurance Group, LLC

5448 Apex Peakway Drive, Ste. 101

Apex, NC 27502

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Secure Access Family Version 6.4. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: Juniper Networks Secure Access Family Version 6.4
ST Revision	1.9
ST Publication Date	February 26, 2010
Author	Juniper Networks and Apex Assurance Group

1.2 TOE Reference

TOE Reference	Juniper Networks Secure Access Family Version 6.4R2.0

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
NTP	Network Time Protocol
OSP	Organizational Security Policy
RFC	Request for Comment
RSA	Rivest Shamir Adelman
SA	Security Association
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell

TERM	DEFINITION
SSL	Secure Sockets Layer
ST	Security Target
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Function
VPN	Virtual Private Network

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview

The TOE is Juniper Networks Secure Access Family Version 6.4 running software version 6.4R2.0. The TOE provides secure remote access to internal network resources, such as:

- Web-based traffic, including Web pages and Web-based applications
- Java applets, including Web applications that use Java applets.
- File traffic, including file servers and directories
- Client/server applications
- Telnet and SSH terminal emulation sessions
- Windows Terminal Servers and Citrix server terminal emulation sessions
- E-mail clients based on the IMAP4, POP3, and SMTP protocols
- All network traffic

Secure Access acts as a secure application-layer gateway that intermediates all requests between remote computers and internal corporate resources. All requests from remote computers to a Secure Access appliance and from a Secure Access appliance to remote computers are encrypted using SSL/HTTPS 168-bit encryption. All unencrypted requests (e.g. HTTP) are redirected to HTTPS, which ensures the connection is encrypted. Each request is subject to administratively defined access control and authorization policies, such as dual-factor or client-side digital certificate authentication, before the request is forwarded to an internal resource. Users gain authenticated access to authorized resources via an extranet session hosted by the appliance. From any Internet-connected Web browser, users can access Web-based enterprise applications, Java applications, file shares and terminal hosts.

1.7 TOE Description

1.7.1 Physical Boundary

The TOE physical boundary is the respective appliance. The TOE is completely self-contained, housing the software and hardware necessary to perform all functions. The TOE has two logical interfaces: end

user and admin interface. The admin interface to the TOE includes both a terminal console and a Web-Based administrative interface. The end user interfaces to the TOE using a Web-Based user interface.

The TOE includes a proprietary web server developed by Juniper, which is part of the Secure Content Server and provides the main interface for both users and administrators of the TOE. The web server provides users an interface to submit connection requests via an HTTPS encrypted tunnel. The web server provides administrators an interface to administrate the TOE using a web browser. The web server component is included as part of the TOE.

The TOE also utilizes a Linux operating system that is based on the Red Hat Linux 7.3 distribution and includes the 2.6.11.1 kernel. The operating system is relied upon for all access to the physical hardware devices connected to the TOE and for providing reliable time stamping.

The TOE is a combined hardware/software TOE and is defined as the Secure Access Family Version 6.4. The TOE boundary is shown below:

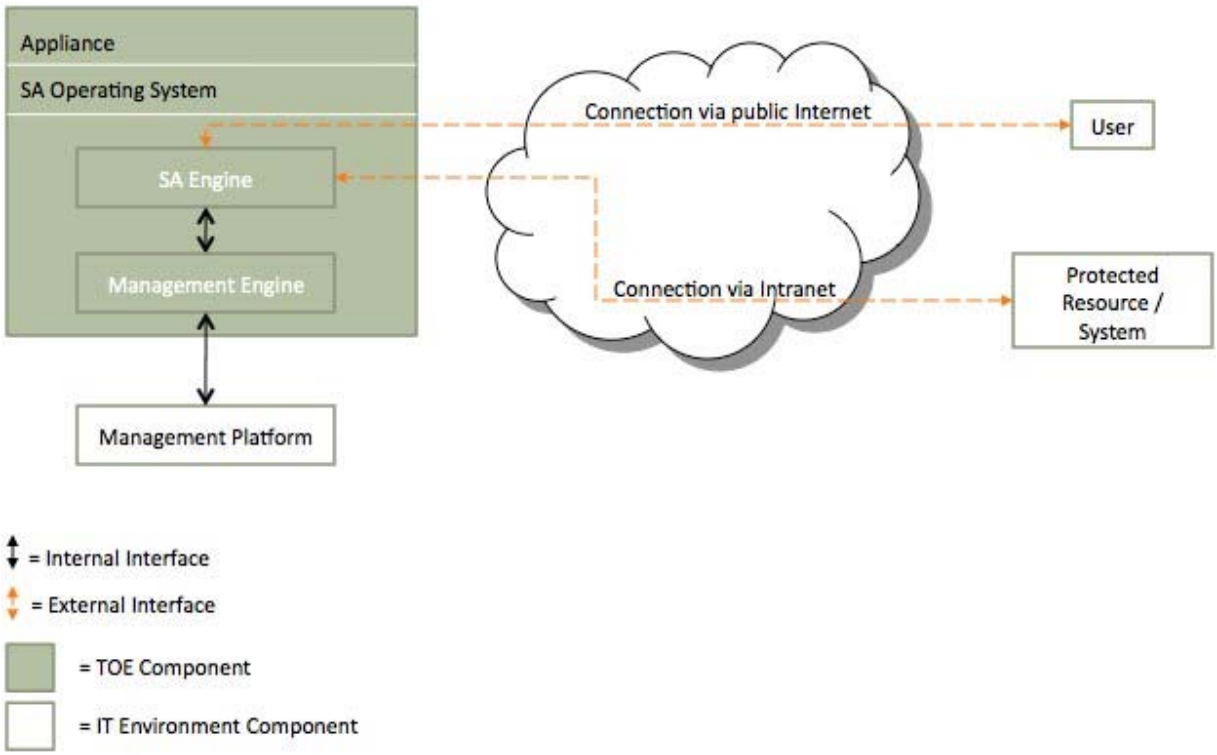

Figure 1 – TOE Boundary

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
Software	Version 6.4R2.0
Hardware	Secure Access 700, 2000, 2500, 4000, 4500, 4500 FIPS, 6000, 6000SP, 6500, 6500 FIPS

Table 3 – Evaluated Configuration for the TOE

The TOE interfaces are comprised of the following:

1. Network interfaces which pass traffic
2. Management interface through which handle administrative actions.

1.7.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	Secure Access generates audit records for security events. The administrator and read-only administrator are the only roles with access to the audit trail and have the ability to view the audit trail.
Cryptographic Support	Secure Access supports secure communications between users and the TOE. This encrypted traffic prevents modification and disclosure of user information.
User Data Protection	Secure Access provides an information flow security policy. The security policy limits traffic to URLs and resource types, such as file servers, to specific user roles.
Identification and Authentication	All users are required to perform identification and authentication before any information flows are permitted. Additionally, administrators must be authenticated before performing any administrative functions.
Security Management	Secure Access provides a wide range of security management functions. Administrators can configure the TOE, manage users, the information flow policy, and audit among other routine maintenance activities.

Table 4 – Logical Boundary Descriptions

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL3 assurance package augmented with ALC_FLR.2 defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behavior of TSF data without being detected.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between a remotely located authorized administrator and the TOE.
T.REPLAY	An unauthorized person may replay valid identification and authentication data obtained while monitoring the TOE's network interface to access functions provided by the TOE.

THREAT	DESCRIPTION
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

Table 5 – Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

3.2 Organizational Security Policies

The TOE is not required to meet any organizational security policies.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.PHYSEC	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 6 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator and/or user through encryption.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.MEDIAT	The TOE must mediate the flow of all information from users on an external network to resources on an internal network, and must ensure that residual information from a previous information flow is protected and not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.SECKEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

Table 7 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMTRA	Authorized administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

OBJECTIVE	DESCRIPTION
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.PUBLIC	The TOE does not host public data.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 8 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.AUDACC	T.AUDFUL	T.MEDIAT	T.NOAUTH	T.OLDINF	T.PROCOM	T.REPLAY	T.SELPRO	T.TUSAGE	A.GENPUR	A.NOEVIL	A.PHYSEC	A.PUBLIC	A.SINGEN
O.ACCOUN	✓													
O.AUDREC	✓													
O.ENCRYP						✓								
O.IDAUTH				✓										
O.MEDIAT			✓		✓									
O.SECFUN		✓												
O.SECKEY						✓								
O.SECSTA								✓						
O.SELPRO		✓						✓						
O.SINUSE							✓							
OE.ADMTRA									✓		✓			
OE.GENPUR										✓				
OE.GUIDAN									✓					
OE.PHYSEC												✓		
OE.PUBLIC													✓	
OE.SINGEN														✓

Table 9 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.AUDACC	This threat is completely countered by • O.ACCOUN which ensures the TOE provides user accountability for information flows through the TOE and for Administrator use of security functions related to audit. • O.AUDREC which ensures The TOE provides a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes
T.AUDFUL	This threat is completely countered by • O.SECFUN which ensures the TOE provides functionality that enables an Administrator to use the TOE security functions and also ensures that only Administrators are able to access such functionality • O.SELPRO which ensures the TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
T.MEDIAT	This threat is completely countered by • O.MEDIAT which ensures the TOE mediates the flow of all information from users on an external network to resources on an internal network
T.NOAUTH	This threat is completely countered by • O.IDAUTH which ensures the TOE uniquely identifies and authenticates the claimed identity of all users before granting a user access to TOE functions.
T.OLDINF	This threat is completely countered by • O.MEDIAT which ensures that residual information from a previous information flow is protected and not transmitted
T.PROCOM	This threat is completely countered by • O.ENCRYP which ensures the TOE protects the confidentiality of its dialogue with an Administrator through encryption • O.SECKEY which ensures the TOE provides the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows
T.REPLAY	This threat is completely countered by • O.SINUSE which the TOE prevents the reuse of authentication data for users attempting to authenticate at the TOE from a connected network
T.SELPRO	This threat is completely countered by • O.SECSTA which ensures the TOE does not compromise its resources or those of any connected network upon initial start-up or recovery from an interruption in TOE service • O.SELPRO which ensures the TOE protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions

THREAT	RATIONALE
T.TUSAGE	This threat is completely countered by • OE.ADMTRA which ensures the operational environment provides well-trained administrators to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE. • OE.GUIDAN which ensures the operational environment provides a secure manner of TOE delivery, installation, administration, and operation

Table 10 – Mapping of Objectives to Threats

4.3.1.2 Rationale for Security Objectives of the TOE

OBJECTIVE	RATIONALE
O.ACCOUN	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that administrators, read-only administrators, and user admins are accountable for the use of security functions related to audit.
O.AUDREC	This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search the information contained in the audit trail.
O.ENCRYP	This security objective is necessary to counter the threat T.PROCOM by requiring that an administrator, read-only administrator, and user admin use encryption when performing administrative functions on the TOE remotely.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
O.SECFUN	This security objective is necessary to counter the threat T.AUDFUL by requiring that the TOE provides functionality that ensures that only the administrator, read-only administrator, and user admin has access to the TOE security functions.
O.SECKEY	The objective mitigates the threat of data modification or disclosure by ensuring that cryptographic keys are generated sufficiently, kept confidential, and destroyed property (T.PROCOM)
O.SECSTA	This security objective ensures that no information is comprised by the TOE upon startup or recovery and thus counters the threat T.SELPRO.
O.SELPRO	This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

OBJECTIVE	RATIONALE
O.SINUSE	This security objective is necessary to counter the threats: T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
OE.ADMTRA	This non-IT security objective is necessary to counter the threat T.TUSAGE and support the assumption A.NOEVIL because it ensures that authorized administrators receive the proper training in the correct configuration, installation and usage of the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.PHYSEC	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.PHYSEC).
OE.PUBLIC	The TOE does not host public data.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 11 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

There are no extended components in this Security Target.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in case of possible audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
	FDP_RIP.1	Subset Residual Information Protection
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SAE.1	Time-limited authorization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_STM.1	Reliable Time Stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channels	FTP_TRP.1	Trusted Path

Table 12 – TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 – Audit Data Generation

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

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

b) All auditable events for the [*not specified*] level of audit; and

c) [The events in column two of Table 13 – Auditable Events]

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

a) Date and time of the event, type of event, subject 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 13 – Auditable Events].

SFR	EVENT	DETAILS
FMT_SMR.1	Modifications to the group of users that are part of a role.	The identity of the Administrator performing the modification and the user identity being associated with a role
FIA_UID.2	All use of the user identification mechanism.	None
FIA_UAU.2	Any use of the user authentication mechanism.	None
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the Administrator performing the operation

SFR	EVENT	DETAILS
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit with the exception for viewing information flow security policy rules (FMT_MOF.1 b), user attribute values (FMT_MOF.1 c), and audit trail data (FMT_MOF.1 f).	The identity of the Administrator performing the operation

Table 13 – Auditable Events

6.1.1.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [an Administrator and Read-only Administrator roles] with the capability to read [all audit information] from the audit records.

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

6.1.1.3 FAU_STG.1 – Protected Audit Trail Storage

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

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

6.1.1.4 FAU_STG.3 – Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall take [action to generate an audit record when the audit trail reaches 90% full and when it is completely full and overwrite the oldest stored audit records with new audit records] if the audit trail exceeds [200 MB].

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [ANSI X9.31] and specified cryptographic key sizes [128-, 192-, or 256-bit AES key and 168-bit TDES key] that meet the following: [FIPS 197 for AES and FIPS 46-3 for TDES].

6.1.2.2 FCS_CKM.2 – Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA] that meets the following: [RSA_WITH_3DES_CBC_SHA or RSA_WITH_AES_CBC_SHA in the TLS specification in RFC 2246].

6.1.2.3 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [Federal Information Processing Standard 140 requirements for key zeroization].

6.1.2.4 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [the operations described below] in accordance with a specified cryptographic algorithm [multiple algorithms in the modes of operation described below] and cryptographic key sizes [multiple key sizes described below] that meet the following: [multiple standards described below].

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	STANDARDS
Encryption and Decryption	AES (CBC mode)	128, 192, 256	FIPS 197
	TDES	168	FIPS 46-3
Hashing	SHS (SHA-1)	160 (size of digest)	FIPS 180-2
	MD5	128	RFC 1321
Random Number Generation	ANSI X9.31	Not Applicable	ANSI X9.31
Digital Signatures	RSA	Modulus Size: 1024	PKCS7

Table 14 – Cryptographic Operations

6.1.3 Information Flow Control (FDP)

6.1.3.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [Authenticated User SFP] on

[Subjects: unauthenticated external IT entities that send and receive packets through the TOE to one another,

Information: network packets sent through the TOE from one subject to another, and

Operations: permit, deny, or reject routing of information].

6.1.3.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [Authenticated User SFP] based on the following types of subject and information security attributes:

[Subject security attributes:

- Role

Information security attributes:

- Destination URL;
- Resource type].

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

[

- A user's role is permitted to access the requested URL, or
- A user's role is permitted to access the requested resource type].

FDP_IFF.1.3 The TSF shall enforce the [No additional rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [No additional rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [No additional rules].

6.1.3.3 FDP_RIP.1 – Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] the following objects: [users].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [identity, association of a human user with a role, password].

6.1.4.2 FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

1. Minimum of eight (8) characters,
2. Minimum of three (3) numeric characters,
3. Minimum of three (3) alphabetic characters,
4. Combination of both uppercase and lowercase alphabetic characters,
5. Different from the username, and
6. Different from the previously used password].

6.1.4.3 FIA_UAU.2 – User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.4 FIA_UID.2 – User Identification before Any Action

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

6.2 Security Management (FMT)

6.2.1.1 FMT_MOF.1 – Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [

1. Start-up and shutdown;
2. Create, delete, modify, and view information flow security policy rules that permit or deny information flows;

3. Create, delete, modify, and view user attribute values defined in FIA_ATD.1;
4. Enable and disable external IT entities from communicating to the TOE;
5. Modify and set the time and date;
6. Archive, clear, and review the audit trail;] to [the Administrator role].

6.2.1.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Authenticated User SFP] to restrict the ability to [*query, modify, delete*] the security attributes [information flow security policy rules that permit or deny information flows and user attribute values defined in FIA_ATD.1] to [the Administrator role].

6.2.1.3 FMT_MSA.2 – Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [security attributes listed with Authenticated User SFP].

6.2.1.4 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Authenticated User 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 [the Administrator role] to specify alternative initial values to override the default values when an object or information is created.

6.2.1.5 FMT_SAE.1 – Time-limited Authorization

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [passwords] to [the Administrator role].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [prompt the authenticated entity to change their password before allowing access to the User or Administrator interfaces of the TOE] after the expiration time for the indicated security attribute has passed.

6.2.1.6 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **control** the [data described in the table below] to [the Administrator role]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE	CLEAR
Authenticated User SFP	✓	✓	✓	✓	✓
User Account Attributes			✓		
Audit Logs				✓	
Date/Time			✓		
Rules that restrict the ability to establish management sessions			✓		

Table 15 – Management of TSF data

6.2.1.7 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Start-up and shutdown;

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

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

d) Enable and disable external IT entities from communicating to the TOE;

e) Modify and set the time and date;

f) Archive, clear, and review the audit trail].

6.2.1.8 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [User, User Admin, Administrator, and Read-Only Administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.3 TOE Access (FTA)

6.2.3.1 FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [10 minute period of inactivity or a 60 minute maximum session period has been reached].

6.2.4 Trusted Path/Channels (FTP)

6.2.4.1 FTP_TRP.1 –Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data [*from modification or disclosure*].

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*initial user authentication*, [and all further communication after authentication].

6.3 Security Functional Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

6.4 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.5.3 – Security Assurance Requirements.

6.5 Security Requirements Rationale

6.5.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SECKEY	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.SINUSE
FAU_GEN.1							✓	✓		
FAU_SAR.1							✓			
FAU_STG.1						✓			✓	
FAU_STG.3						✓			✓	
FCS_CKM.1				✓						
FCS_CKM.2				✓						
FCS_CKM.4				✓						
FCS_COP.1					✓					
FDP_IFC.1		✓								
FDP_IFF.1		✓								
FDP_RIP.1		✓								
FIA_ATD.1	✓									✓
FIA_SOS.1	✓									
FIA_UAU.2	✓									
FIA_UID.2	✓							✓		
FMT_MOF.1			✓						✓	
FMT_MSA.1		✓	✓		✓				✓	
FMT_MSA.2		✓	✓		✓				✓	
FMT_MSA.3		✓	✓		✓				✓	
FMT_MTD.1	✓	✓	✓		✓				✓	
FMT_SAE.1									✓	
FMT_SMF.1									✓	
FMT_SMR.1									✓	
FPT_STM.1							✓			
FTA_SSL.3						✓				
FTP_TRP.1					✓					

Table 16 – Mapping of TOE Security Functional Requirements and Objectives

6.5.2 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
FAU_SAR.1	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.
FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering. Only the Administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
FAU_STG.3	This component ensures that the authorized administrator will be able to save data contained in the audit trail if the storage space should become full. It also ensures that no current audit events are lost. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
FCS_CKM.1	This component ensures that cryptographic keys and parameters are generated with standards-based algorithms (O.SECKEY).
FCS_CKM.2	This component provides secure key distribution to remote trusted IT products (users or other instances of TOE). The TOE to perform authentication using digital certificates, ensuring the source is trusted (O.SECKEY).
FCS_CKM.4	This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications (O.SECKEY).
FCS_COP.1	This component ensures that when all users communicate with the TOE remotely from an internal or external network that robust algorithms are used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.
FDP_IFC.1	This component identifies the entities involved in the Authenticated User SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_IFF.1	This component identifies the attributes of the users sending and receiving the information in the Authenticated User SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_RIP.1	This component ensures that any residual information content pertaining to a resource accessible by a user, such as access to a file server, is not made available upon the allocation of that resource to another user. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

SFR	RATIONALE
FIA_SOS.1	This component exists to ensure that passwords generated by users can be verified to meet the defined minimum password strength requirements. This component traces back to and aids in meeting the following objective: O.IDAUTH.
FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and as such aids in meeting O.IDAUTH.
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and as such aids in meeting O.IDAUTH and O.ACCOUN.

SFR	RATIONALE
FMT_MOF.1	This component was chosen to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.SECSTA.
FMT_MSA.1	This component restricts the ability to modify, delete, or query the parameters for the Authenticated User SFP to an Administrator, and as such aids in meeting O.ENCRYP. It also assists in effective management, and as such aids in meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_MSA.2	This component ensures that only secure values are accepted for the configuration parameters associated with the Authenticated User SFP, and as such aids in meeting O.ENCRYP. It also assists in effective management, and as such aids in meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_MSA.3	This component ensures that the TOE provides a default restrictive policy for the information flow control security rules, yet allows an Administrator to override the default restrictive values with permissive values. This component traces back to and aids in meeting the following objectives: O.ENCRYP, O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_MTD.1	This component restricts the ability to modify the Authenticated User SFP, and as such aids in meeting O.ENCRYP, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.IDAUTH, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to delete audit logs, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify the date and time, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_SAE.1	The component provides the capability for an Administrator to specify an expiration time on a user's password. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMF.1	This component was chosen in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to an authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_STM.1	FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

SFR	RATIONALE
FTA_SSL.3	This component protects the TOE's communication path by terminating sessions idled for longer than 10 minutes and terminating sessions lasting longer than 60 minutes. This component traces back to and aids in meeting the following objective: O.SELPRO
FTP_TRP.1	This component works with the encryption provided in the FCS_COP.1 requirement to ensure that user authentication data or other user data is protected from disclosure and modification. This component traces back to and aids in meeting the following objective: O.ENCRYP.

Table 17 – Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.ACCOUN	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited • FIA_UID.2 ensures that users are identified to the TOE
O.AUDREC	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited • FAU_SAR.1 which requires that the audit trail can be read • FPT_STM.1 ensures that reliable time stamps are provided for audit records
O.ENCRYP	This objective is completely satisfied by • FCS_COP.1 which ensures robust algorithms are used to support encrypted communications between users and Secure Access • FMT_MSA.1 which restricts the ability to modify, delete, or query the parameters for the Authenticated User SFP to an Administrator • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Authenticated User SFP • FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations • FTP_TRP.1 which ensures all communications between users and Secure Access is encrypted via a secure connection using encryption & decryption algorithms

OBJECTIVE	RATIONALE
O.IDAUTH	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE • FIA_UID.2 which ensures that users are identified to the TOE • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations
O.MEDIAT	This objective is completely satisfied by • FDP_IFC.1 which ensures the TOE supports an authenticated user information flow policy that controls who can send and receive network traffic • FDP_IFF.1 which ensures Authenticated User SFP limits information flow based on user roles and resource types • FDP_RIP.1 which ensures the TOE tracks all packet information including packet length and ensures that no residual data is exposed to users • FMT_MSA.1 which restricts the ability to modify, delete, or query the parameters for the Authenticated User SFP to an Administrator • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Authenticated User SFP • FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations

OBJECTIVE	RATIONALE
O.SECFUN	This objective is completely satisfied by • FAU_STG.1 which ensures only the authorized administrator has access to the logs • FAU_STG.3 which ensures the TOE overwrites the oldest stored audit data with any further audit data generated when the audit trail becomes full • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to an Administrator • FMT_MSA.1 which restricts the ability to modify, delete, or query the parameters for the Authenticated User SFP to an Administrator • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Authenticated User SFP • FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations • FMT_SAE.1 which allows the Administrator to set expiration times for user passwords • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.
O.SECKEY	This objective is completely satisfied by • FCS_CKM.1 which ensures that cryptographic keys and parameters are generated with standards-based algorithms • FCS_CKM.2 which provides secure key distribution to remote trusted IT products • FCS_CKM.4 which ensures that the cryptographic keys and parameters are safely destroyed.
O.SECSTA	This objective is completely satisfied by • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to an authorized Administrator • FMT_MSA.1 which restricts the ability to modify, delete, or query the parameters for the Authenticated User SFP to an Administrator • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Authenticated User SFP • FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations

OBJECTIVE	RATIONALE
O.SELPRO	This objective is completely satisfied by • FAU_STG.1 which ensures only the authorized administrator has access to the logs • FAU_STG.3 which ensures the TOE overwrites the oldest stored audit data with any further audit data generated when the audit trail becomes full • FTA_SSL.3 which protects existing encrypted sessions from becoming compromised by enforcing a session timeout when certain conditions are met
O.SINUSE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users

Table 18 – Rationale for TOE Objectives to SFRs

6.5.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.2 Flaw Reporting Procedures. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation 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
ATE: Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 19 – Security Assurance Requirements at EAL3

6.5.4 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3 augmented with ALC_FLR.2. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides

the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.5.5 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Juniper Networks Secure Access Family Version 6.4
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: Juniper Networks Secure Access Family Version 6.4
ADV_TDS.2 Architectural Design	Architectural Design: Juniper Networks Secure Access Family Version 6.4
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Secure Access Family Version 6.4
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Secure Access Family Version 6.4
ALC_CMC.3 Authorization Controls	Security Measures: Juniper Networks Secure Access Family Version 6.4
ALC_CMS.3 Implementation representation CM coverage	Security Measures: Juniper Networks Secure Access Family Version 6.4
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Juniper Networks Secure Access Family Version 6.4
ALC_DVS.1 Identification of Security Measures	Security Measures: Juniper Networks Secure Access Family Version 6.4
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Model: Juniper Networks Secure Access Family Version 6.4
ALC_FLR.2 Flaw Reporting Procedures	Flaw Reporting Procedures: Juniper Networks Secure Access Family Version 6.4
ATE_COV.2 Analysis of Coverage	Testing Evidence Supplement: Juniper Networks Secure Access Family Version 6.4
ATE_DPT.1 Testing: Basic Design	Testing Evidence Supplement: Juniper Networks Secure Access Family Version 6.4
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: Juniper Networks Secure Access Family Version 6.4

Table 20 – Security Assurance Rationale and Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Operations
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

7.2 Security Audit

Secure Access generates a fine-grained set of audit log. These logs are stored locally, and the system can also send them to an external SYSLOG server for alternative storage. The logs are divided into the following categories and are maintained separately:

- Event logs – used to track system related events such as start-up and shutdown
- Admin access logs – used to record administrator generated events
- User access logs – record user access events such as retrieving a file.

Each log contains the following fields:

- Severity (Info/Minor/Major)
- ID
- Timestamp
- Date
- Event outcome (success or failure)
- Entity who initiated the activity : [initiating IP] initiator username if applicable, (user type if applicable),[user role if applicable]
- Description of the activity

The TOE generates logs for the following list of events:

- Modifications to the group of users that are part of a role, which includes the identity of the Administrator performing the modification and the user identity being associated with a role in each related log;
- All use of the user identification mechanism, which includes the user identities provided to the TOE in each related log;
- Any use of the authentication mechanism, which includes the user identities provided to the TOE in each related log;
- All decisions on requests for information flow with the exception for permitted access to a Windows file resource, which includes the presumed addresses of the source and destination subject in each related log;
- Changes to the time, which includes the identity of the Administrator performing the operation in each related log;
- Use of the functions listed in this requirement pertaining to audit with the exception for viewing information flow security policy rules (FMT_MOF.1 b), user attribute values (FMT_MOF.1 c), and audit trail data (FMT_MOF.1 f), which includes the identity of the Administrator performing the operation in each related log.

The logs are only accessible through the Web-Based administrative interface, which only authenticated Administrators are authorized access. Administrators can view, clear, save the logs. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based administrative interface. The administrator also has the ability to change the log settings.

Secure Access maintains a circular buffer for audit records. After the audit log fills, the oldest audit records are overwritten.

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

- FAU_GEN.1: Secure Access generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details.
- FAU_SAR.1: The Administrator has the ability to read all of the audit logs. Each log is presented to the administrator in a human-readable format.
- FAU_STG.1: Only the Administrator has access to the logs. The Administrator is not permitted to modify any information in the logs. The only manipulations allowed on logs are to clear them, download them, save them, or view them.
- FAU_STG.3: When the audit logs reach 90% full, Secure Access generates an audit event indicating that the log in question (i.e. Event Log, User Access Log, Admin Access Log) is full. When the audit logs reach 200MB, Secure Access generates an audit event indicating that the log in question (i.e. Event Log, User Access Log, Admin Access Log) is full and overwrites the oldest stored audit data with any further audit data generated. The default setting for the audit log size is 200MB. However, the size of the log can be configured up to 500MB.

7.3 Cryptographic Support

Secure Access provides an encrypted path between users and the TOE. Users connect to the TOE using a secure connection using TDES or AES encryption algorithms supported by Secure Access. The secure connection ensures that user passwords and data are protected from modification and disclosure.

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: This component ensures that cryptographic keys and parameters are generated with standards-based algorithms
- FCS_CKM.2: This component provides secure key distribution to remote trusted IT products
- FCS_CKM.4: This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys
- FCS_COP.1: Robust algorithms are used to support encrypted communications between users and Secure Access.

7.4 User Data Protection

Secure Access enforces an information flow policy between authenticated users and protected resources logically behind the appliance. Before any access is granted, users must log into Secure Access. Each user account is associated with one or more user roles. The administrator sets up roles and access rules associated with the roles. The access rules can address URLs or resource types. URL rules permit specific user roles to access specific URLs. Rules can be specified using exact URLs or URLs can contain wildcard designations. The last type of rule is based on rules that permit specific user roles to access specific resources such as file servers or web servers.

Secure Access ensures that all packets that are delivered to a user do not contain residual information. To ensure this, The Secure Access appliance interprets every byte in a complete information stream from the first packet to the last. All temporary storage is accounted for in that the size of a temporary storage relative to every packet is known.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE supports an authenticated user information flow policy that controls who can send and receive network traffic.
- FDP_IFF.1: The Authenticated User SFP limits information flow based on user roles and resource types. Administrators have the ability to establish rules that permit or deny information flows based on the combination of attributes listed.
- FDP_RIP.1: The TOE tracks all packet information including packet length and ensures that no residual data is exposed to users.

7.5 Identification and Authentication

Secure Access performs identification and authentication of all users and administrators accessing the TOE. Secure Access has the ability to authenticate users locally using a password or can integrate with a remote authentication server. In the evaluated configuration, Secure Access will perform the authentication locally. Users enter a username and password, which is validated by Secure Access against the user information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

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

- FIA_ATD.1: For each registered user, the TOE stores the following information: user identity, user name, user roles, and password.
- FIA_SOS.1: The TOE is equipped with a mechanism that can be configured by the administrator to verify that user authentication secrets meet a list of criteria for ensuring their strength. The following parameters for authentication secrets are required for the evaluated configuration: a minimum of eight (8) characters, a minimum of three (3) numeric characters, a minimum of three (3) alphabetic characters, a combination of both uppercase and lowercase alphabetic characters, different from the username, and different from the previously used password.
- FIA_UAU.2: The TOE requires a valid password associated with a user name before providing access to the TOE. Passwords must conform to the requirements in FIA_SOS.1
- FIA_UID.2: The TOE requires a user name during the identification and authentication process. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username.

7.6 Security Management

Secure Access provides security management functions via a browser interface. The Administrator logs onto the TOE from a protected network and performs all management functions through the browser interface. The Administrator has the ability to control all aspects of the Secure Access configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

Secure Access also provides a console port for certain management capabilities, such as configuring the network relevant information pertaining to the internal and external network interfaces. However, the console port does not provide the management capabilities necessary to utilize the security management functionalities claimed within this ST.

Administrators set the information flow policy rules on a per user basis. When the Administrator adds a new user, the Administrator defines the user access. Although users are grouped into roles,

Administrators can create rules that except specific users from the constraints of their role. By default, user access is restrictive but the Administrator may override the default upon rule creation.

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

- FMT_MOF.1: The ability to perform the following security management functions is restricted to an Administrator role:
  a) start-up and shutdown of Secure Access;
  b) create, delete, modify, and view resource policy rules that permit or deny resource requests;
  c) create, delete, modify, and view user attribute values, which include a user's identity, association to a role, and authentication credentials;
  d) enable and disable external IT entities from communicating to the TOE;
  e) modify and set the time and date;
  f) archive, clear, and review the audit trail.

- FMT_MSA.1: This component restricts the ability to modify, delete, or query the parameters for the Authenticated User SFP to the Administrator role
- FMT_MSA.2: This component ensures that only secure values are accepted for the configuration parameters associated with the Authenticated User SFP
- FMT_MSA.3: The TOE allows restrictive access by default but the Administrator role can assign more restrictive permissions.
- FMT_MTD.1: The TOE restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations. All restrictions apply to unauthenticated or unauthorized users.
- FMT_SAE.1: The TOE allows the Administrator role to set expiration times for user passwords. When these times are exceeded a user is prompted to change their password before being allowed additional access to the TOE.
- FMT_SMF.1: The TOE supports the following security management functions:

  a) start-up and shutdown of Secure Access;
  b) create, delete, modify, and view resource policy rules that permit or deny resource requests;
  c) create, delete, modify, and view user attribute values, which include a user's identity, association to a role, and authentication credentials;
  d) enable and disable external IT entities from communicating to the TOE;
  e) modify and set the time and date;
  f) archive, clear, and review the audit trail.

- FMT_SMR.1: The TOE supports the roles administrator, read-only administrator, user, and user admin. The administrator role provides a user within the administrator's authentication realm access to perform all management functionalities available from within the Administrator Console. The administrator dynamically sets up user roles and access rules associated with the roles. The read-only administrator role provides a user within the administrator's authentication realm read-only access to the various configurations and logs available from within the Administrator Console. The user and user admin roles provide a user within the user's authentication realm access to initiate an information flow request and access internal resource, if permitted. Additionally, the user admin role allows a user within the user's authentication realm to create, modify or delete existing user's within the user's authentication realm. Users within the administrator's authentication realm are only permitted to access the TOE via the Administrator Console. Users within the user's authentication realm are only permitted to access the TOE via the End-User Interface.

7.7 Protection of the TSF

Secure Access provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware.

Secure Access protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 10 minutes or reaches a maximum lifetime of 60 minutes, the session times out and is deleted from the session table. Session timeouts are enforceable on sessions initiated on both the administrator and user interfaces of the TOE.

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

- FPT_STM.1: The TOE generates a reliable timestamp for its own use.
- FTA_SSL.3: The TOE protects existing encrypted sessions from becoming compromised by enforcing a session timeout after a session has been idle for more than 10 minutes or after a maximum session lifetime of 60 minutes has been reached, whichever comes first.
- FTP_TRP.1: All communications between users and Secure Access is encrypted via a secure connection using encryption & decryption algorithms defined in FCS_COP.1. This protects the traffic from disclosure and modification.