Juniper Networks Secure Access Family 5.1R2

Security Target

Version 1.1

2/2/2006

Prepared for:
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

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 consists of a series of Juniper Networks Secure Access, Release 5.1R2 appliances. Secure Access provides secure remote access to internal network resources. Secure Access can provide secure remote access to a variety of resources, such as:

- Messaging clients such as Microsoft Outlook and Lotus Notes servers
- Email servers
- Terminal-based applications (IBM 3270, VT100)
- Corporate file servers
- Web-based enterprise applications
- Intranet pages

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Juniper Networks Secure Access family 5.1R2 Security Target

ST Version – Version 1.0

ST Date – 2/2/06

TOE Identification – The TOE is identified as Juniper Networks Secure Access family, Release 5.1R2, which consists of one or more of the following Secure Access appliances:

- Juniper Networks SA 2000, Release 5.1R2
- Juniper Networks NetScreen-SA 3000 FIPS, Release 5.1R2
- Juniper Networks SA 4000, Release 5.1R2
- Juniper Networks NetScreen-SA 5000 FIPS, Release 5.1R2
- Juniper Networks SA 6000, Release 5.1R2

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
    - Part 3 Conformant
    - EAL 2 Conformant

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

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

1.3.2 Terminology and Acronyms

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standard Publication
IT	Information Technology
IVE	Instant Virtual Extranet
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

2 TOE Description

The Target of Evaluation (TOE) is Juniper Networks Secure Access, Release 5.1R2, hereafter referred to as Secure Access or SA, which is configured and operated according to the guidance documents identified later in this Security Target.

This following series of appliance models has been included in the evaluation:

- Juniper Networks SA 2000, Release 5.1R2
- Juniper Networks NetScreen-SA 3000 FIPS, Release 5.1R2
- Juniper Networks SA 4000, Release 5.1R2
- Juniper Networks NetScreen-SA 5000 FIPS, Release 5.1R2
- Juniper Networks SA 6000, Release 5.1R2

2.1 TOE Overview

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 a secure HTTPS connection with 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.

2.2 TOE Architecture

Secure Access contains four major components. Together these and other components of the appliance deliver a simple, secure remote access solution within a single machine. The four major components are:

- Content Intermediation Engine
- Protocol Connectors
- Secure Content Server
- System Data Store and Load Balancing System

Figure 2.1: TOE Architecture

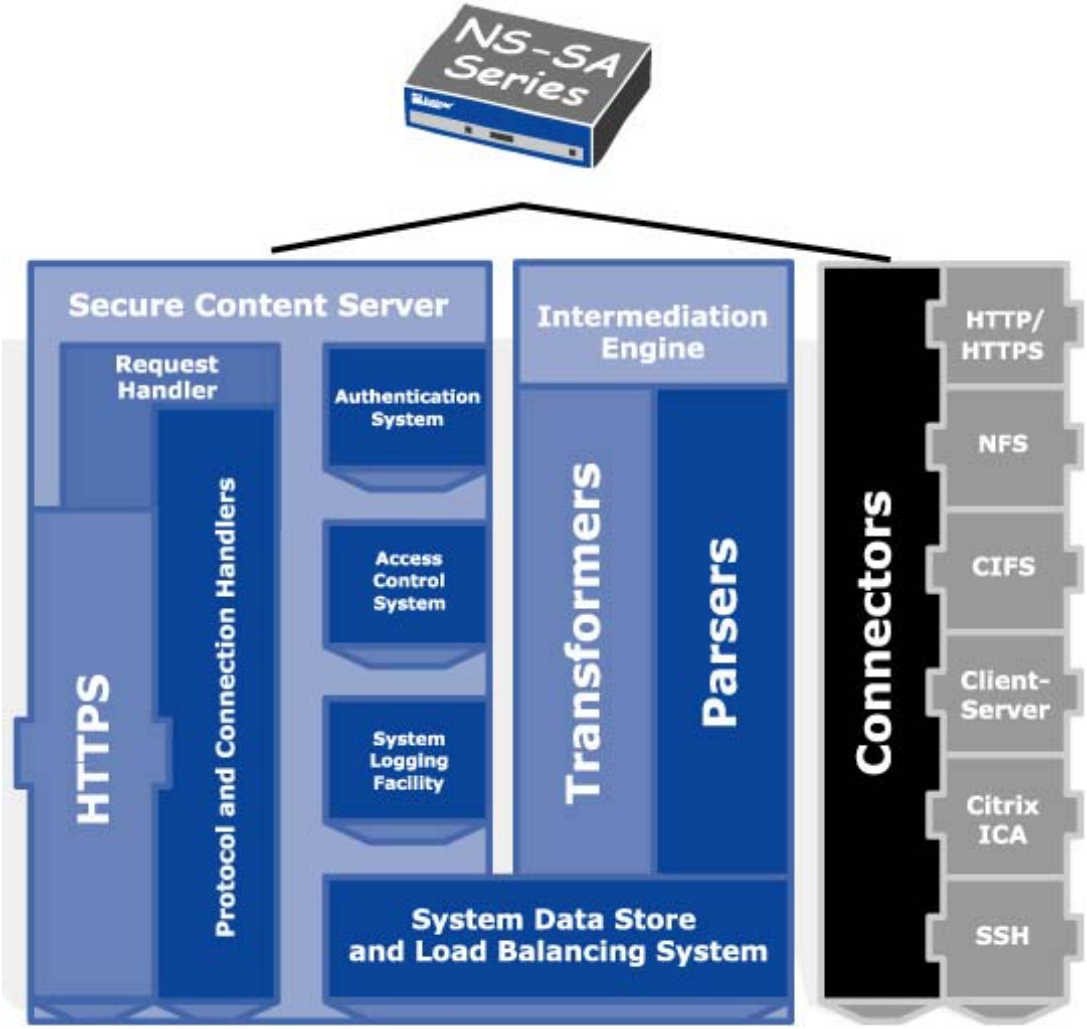


Figure 2.1 shows the SA architecture and the following sections describe each component and its features.

2.2.1 Content Intermediation Engine

The Content Intermediation Engine is the core of Secure Access. It consists of:

- **Parsers** - Event-driven components that process resource data streams and decompose them into "chunks" that are manipulated by associated transformers

- **Transformers** - Components that receive the "chunks." The transformers have the opportunity to modify each chunk in the data stream before writing it out to the Request Handler

- **Connectors** - Components that use protocol adapters to retrieve resource and application data streams, such as documents on file servers, HTML pages on the intranet servers, or messages from an MS Exchange server

Web requests provide the clearest example of the Content Intermediation Engine at work, but generally speaking, support for most content types and application protocols uses a similar approach:

- The file sharing application for remote access to Windows shares and NFS volumes uses a backend connector, and the directory and file meta-data is transformed into a Web view of the volume.
- The client-server application and messaging application support uses backend connectors to communicate with mail servers, messaging servers, and other servers. These messages are transformed into the secure Web protocols before they are written out to the Request Handler.
- The support for Web resources uses a Connector to read HTML and other content streams from an internal HTTP server in addition to a Parser and a Transformer.

2.2.2 Protocol Connectors

Each supported content type has an associated protocol connector. These connectors communicate with the content parsers and with the native content servers. For example, the file share connector communicates with MS Windows file servers through the CIFS protocol over TCP and with UNIX file server through NFS over UDP. In order to enforce native access controls, an additional component connects to the MS NT Domain Controller or UNIX NIS server. Currently Juniper supports connectors for:

- CIFS
- Citrix ICA
- HTTP/HTTPS
- IMAP
- Lotus Notes
- MS MAPI
- NFS
- POP
- SMTP
- Socket-dependent Java applets
- SSH
- Telnet
- URL-dependent Java applets

2.2.3 Secure Content Server

The Secure Content Server provides the core of the security features offered by SA.

The Secure Content Server consists of the following components:

- Access Control System
- Authentication System
- Protocol and Connection Handlers
- Request Handler
- System Logging Facility
- Web Server

The Access Control System provides access control enforcement on requests to resources protected by the TOE. The Access Control System determines if an authenticated user will be allowed or denied access to a requested resource. When an authenticated user makes a request to the backend resources available to the role associated with the authenticated user, the appliance evaluates the corresponding resource policies. A resource policy is a set of resource names (such as URLs and hostnames) to which you grant or deny access or other resource-specific actions, such as rewriting and caching. A resource policy serves as the third level of resource access control. While a role may grant access to certain types of access features and resources (such as bookmarks and applications), whether or not a user can access a specific resource is controlled by resource policies. These policies may even specify conditions that, if met, either deny or grant user access to a server share or file. The administrator dynamically sets up user roles and access rules associated with the roles (see section 6.1.5 for further information)

The Authentication System provides identification and authentication capabilities for authenticating both administrators and users. The Authentication System performs authentication using authentication realms. However, separate authentication databases are used for administrator and user accounts. An authentication realm is a grouping of authentication resources, including:

- An authentication server, which verifies that the user is who he claims to be. An IVE appliance forwards credentials that a user submits on a sign-in page to an authentication server.
- An authentication policy, which specifies realm security requirements that need to be met before an IVE appliance submits a user's credentials to an authentication server for verification.
- A directory server, which is an LDAP server that provides user and group information to an IVE appliance that the appliance uses to map users to one or more user roles.
- Role mapping rules, which are conditions a user must meet in order for an IVE appliance to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

The Protocol and Connection Handlers provide the necessary protocol negotiations to the end user for the specific protocol being used.

The Request Handler runs within the Secure Access appliance. The Request Handler works with the system software and other components to ensure that content can be projected to authorized users in a secure fashion:

- Secure Access uses "cookie trapping." All Web cookies are maintained on the server, and a single session token is transmitted to the Web browser. This feature ensures that no cookie-based session information, stored credentials, or application meta-data leaves the corporate network.
- The Secure Access session token expires when the session becomes idle or the user signs out.
- HTTP headers with all sensitive content contain the Cache-Control directive "no-cache," which prevents them from being stored on the client machine in standard browsers.
- All form fields intermediated by the device includes the autocomplete="off" attribute to prevent values from being stored on the client machine.[1]

The System Logging Facility provides logging capabilities for recording the access decisions resulting from resource requests initiated by authenticated users. The System Logging Facility also provides logging capabilities for recording the access decisions resulting from the actions performed by authenticated administrators.

The Web Server provides an interface to users for using the TOE to access resources protected by the TOE, and provides an interface to administrators for managing the TOE and its security functions. The Web Server also provides the HTTP protocol that is used for both the user and administrator interfaces to receive/transmit and encrypt/decrypt data to or from the TOE.

2.2.4 System Data Store

Administrators can add file, web, and email resources to the TOE during the course of operation. These protected resources are located within the System Data Store. However, Administrators cannot access the protected resources directly and must use the Operating System to transfer resource information. Only the Secure Access Operating System software can access the encrypted data store directly. The operating system uses executable files to provide the storage functions. Users and administrators cannot replace or alter these executable files, as they do not have system-level accounts. This provides separation of duties within the TOE, so potential attackers cannot employ privilege-elevation attacks against the appliance

All data stored on the device is encrypted using AES, however, the protection of the AES encryption is outside of the scope of the TOE.

[1] These are tags that are embedded in the HTTP code. They are not enforced by the TOE, and as such can be over ridden by the user.

2.3 TOE Boundaries

2.3.1 Physical Boundaries

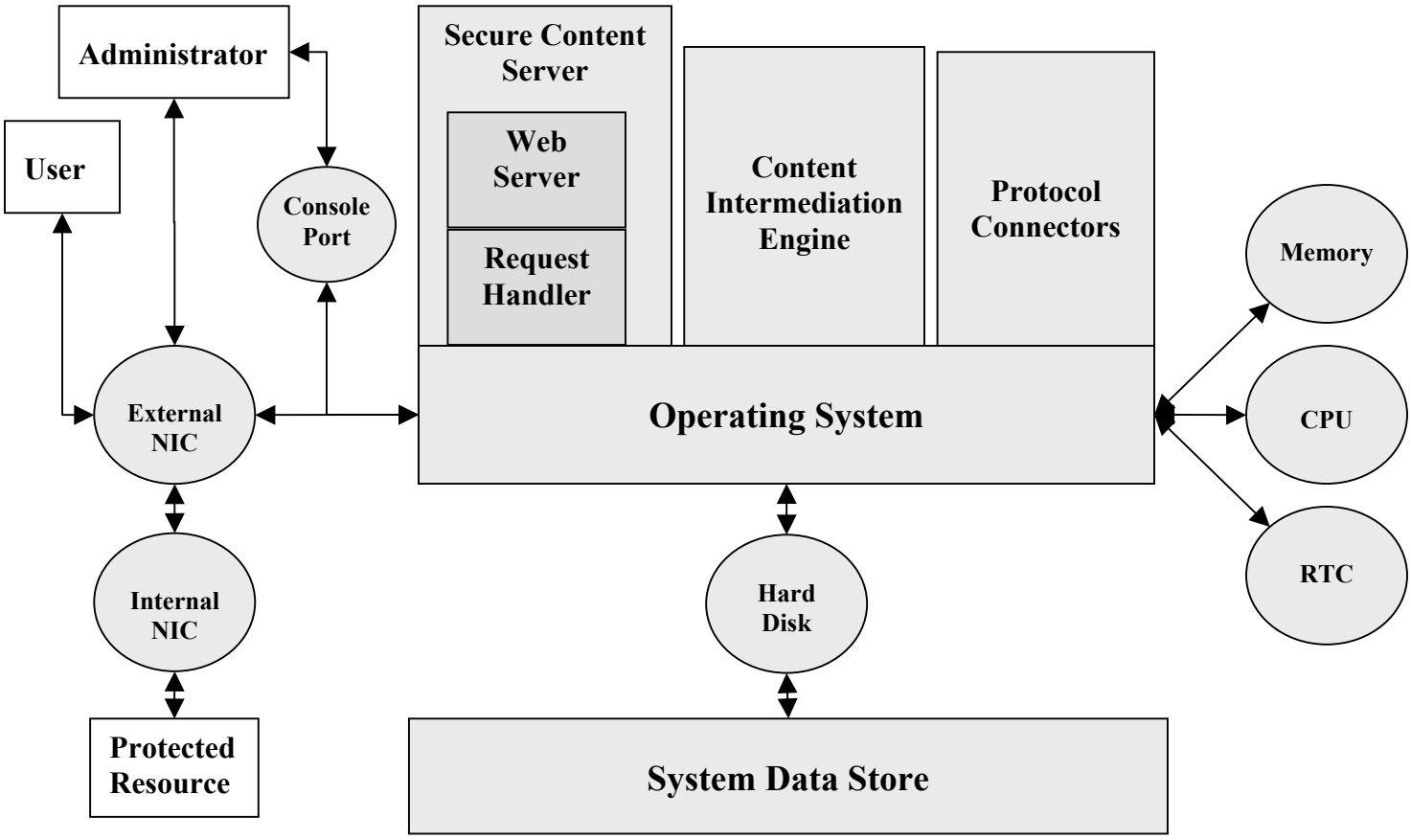
The TOE physical boundary is the appliance itself. The TOE is completely self-contained, housing the software and hardware necessary to perform all functions. The TOE has two logical interfaces: end user and admin interface. The admin interface to the TOE includes both a terminal console and a Web-Based 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 contains the 2.4 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 boundaries are depicted in the following figure. The TOE components are identified with a gray background. The TOE components consist of the Secure Content Server, Web Server, Intermediation Engine, Protocol Connectors, an internal and external Network Interface Card (NIC), Hard Disk, Memory, Central Processing Unit (CPU), System Data Store, Operating System, and Real Time Clock (RTC). The non-TOE components are identified with a white background. These non-TOE components consist of clients and protected resources. Clients exist outside the TOE and connect to the TOE through the external NIC, which is open to the Internet for allowing this connectivity. Protected resources consist of file, web, and email resources, which are added to the TOE by administrators in an operational environment. These protected resources are located within the System Data Store, which is accessible from the internal NIC. Such resources are considered outside the scope of the TOE.

Figure 2.2: TOE Physical Boundaries



2.3.2 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include Security Audit, Cryptography Support, User Data Protection, Identification and Authentication for the administrative functions, the management of the security configurations and the self-protection of the TOE itself.

2.3.2.1 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.

2.3.2.2 Cryptographic support

Secure Access supports secure communications between users and the TOE. This encrypted traffic prevents modification and disclosure of user information.

2.3.2.3 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.

2.3.2.4 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.

2.3.2.5 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.

2.3.2.6 Protection of the TSF

Secure Access protects itself by providing well-defined network interfaces for user access and requiring all users to perform identification and authentication before any information flows are permitted. Additionally, no untrusted software runs on the TOE which ensures the TOE maintains a domain for its own execution.

2.4 TOE Documentation

Juniper Networks offers a series of documents that describe the installation process for Secure Access as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6 for information about these and other documents associated with Secure Access.

3 Security Environment

This section includes the threats addressed by the TOE and the assumptions about its environment. All threats and assumptions were derived from the Traffic Filter Firewall PP[2].

3.1 Threats

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	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

[2] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999

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.
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.

3.2 Assumptions

A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.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.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.PHYSEC	The TOE is physically secure.
A.PUBLIC	The TOE does not host public data.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

4 Security Objectives

This section presents the security objectives for the TOE and its Environment. All objectives were derived from the Traffic Filter Firewall PP[3].

4.1 Security Objectives for the TOE

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 through encryption, if the TOE allows administration to occur remotely from a connected network.

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

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

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 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.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.

[3] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999

4.2 Security Objectives for the Environment

O.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.
O.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
O.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.
O.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
O.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.PHYSEC	The TOE is physically secure.
O.PUBLIC	The TOE does not host public data.
O.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
O.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

5 IT Security Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Secure Access.

Requirement Class	Requirement Component
FAU: 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
FCS: Cryptographic support	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.1: Subset residual information protection
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Specification of secrets
	FIA_UAU.1: Timing of authentication
	FIA_UID.1: Timing of identification
FMT: Security Management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.3: Static attribute initialization
	FMT_SAE.1: Time-limited authorization
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps
	FTP_TRP.1: Trusted Path
	FTA_SSL.3: TSF-initiated termination

Table 1 TOE Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

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

- **a)** Start-up and shutdown of the audit functions;
- **b)** All auditable events for the [*not specified*] level of audit; and
- **c)** **the events in column two of Table 2 Auditable Events**.

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

- **a)** Date and time of the event, type of event, subject identity, 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 2 Auditable Events**.

Functional Requirement	Event	Event Details
FMT_SMR.1	Modifications to the group of users that are part of a role.	The identity of the authorized administrator performing the modification and the user identity being associated with a role
FIA_UID.1	All use of the user identification mechanism.	None
FIA_UAU.1	Any use of the authentication mechanism.	None
FDP_IFF.1[4]	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 authorized administrator performing the operation
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 authorized administrator performing the operation

Table 2 Auditable Events

5.1.1.2 Audit Review (FAU_SAR.1)

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

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

5.1.1.3 Protected audit trail storage (FAU_STG.1)

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

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

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

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**].

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm [**Triple Data Encryption Standard (TDES) as specified in FIPS PUB 46-2 and implementing any mode of operation specified in FIPS PUB 81**] and cryptographic key sizes [**that are 168 binary digits in length**] that meet the following [**FIPS PUB 46-2 and FIPS PUB 81**].

5.1.3 User data protection (FDP)

5.1.3.1 Subset information flow control (FDP_IFC.1)

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

[4] This requirement excludes the capability to audit access permitted to a Windows file resource.

a) subjects: users;
b) information: traffic sent through the TOE from a user on the external network to a resource on the internal network;
c) operation: pass information].

5.1.3.2 Simple security attributes (FDP_IFF.1)

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

a) subject security attributes:
- **Role**

b) 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 provide the following [**no additional rules**].

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [**none**].

5.1.3.3 Subset residual information protection (FDP_RIP.1)

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

5.1.4 Identification and Authentication (FIA)

5.1.4.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users [:

a) identity;
b) association of a human user with a role;
c) password].

5.1.4.2 Verification of secrets (FIA_SOS.1)

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

1. **a minimum of eight (8) characters,**
2. **a minimum of three (3) numeric characters,**
3. **a minimum of three (3) alphabetic characters,**
4. **a combination of both uppercase and lowercase alphabetic characters,**
5. **different from the username, and**
6. **different from the previously used password**].

5.1.4.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow a user to perform certain actions prior to the authentication of the user's identity [**none**]

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.

5.1.4.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow a user to perform certain actions prior to the authentication of the user's identity [none]

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

5.1.5 Security Management (FMT)

5.1.5.1 Management of security functions behavior (FMT_MOF.1)

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

a) start-up and shutdown;
b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;[5]
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;

to **an authorized administrator**].

5.1.5.2 Static attribute initialization (FMT_MSA.3)

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 [**authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.3 Time-limited authorization (FMT_SAE.1)

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [**passwords**] to [**the authorized administrator**].

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.

5.1.5.4 Specification of management functions (FMT_SMF.1)

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].

5.1.5.5 Security roles (FMT_SMR.1)

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

[5] FMT_MOF.1 c) includes the following exceptions: users, user admins, and read-only administrators possess the capability to modify their own password. Additionally, user admins possess the ability to create, modify, and delete users within the user's authentication realm. The modification of a user attribute pertaining to FIA_ATD.1 b) pertains to the association or disassociation of a user to a role.

FMT_SMR.1.2 The TSF shall be able to associate users with [**User, User Admin, Administrator, or Read-Only Administrator**] role.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.6.3 Reliable time stamps (FPT_STM.1)

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

5.1.7 TOE Access (FTA)

5.1.7.1 TSF-initiated termination (FTA_SSL.3)

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**].

5.1.8 Trusted Path/Channels (FTP)

5.1.8.1 Trusted path (FTP_TRP.1)

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**]].

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in the Part 3 Common Criteria version 2.2. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 2 Assurance Components

5.2.1 Configuration management (ACM)

5.2.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labeled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 Development (ADV)

5.2.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1c The presentation of the high-level design shall be informal.
ADV_HLD.1.2c The high-level design shall be internally consistent.
ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

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

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

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

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

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

5.2.5 Tests (ATE)

5.2.5.1 Evidence of coverage (ATE_COV.1)

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

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.6 Vulnerability assessment (AVA)

5.2.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.2.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.3 TOE Strength of Function Claims

5.3.1 Minimum Strength of Function Claim

The TOE claims a minimum strength of function level of SOF-medium for all of the TOE security functional requirements with the exception of FCS_COP.1 because it pertains to cryptography and the assessment of algorithmic strength does not form part of the evaluation.

5.3.2 Explicit Strength of Function Claims

The TOE claims an explicit strength of function level of SOF-medium for the security functional requirements FIA_SOS.1.

6 TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

The Identification and Authentication security function implements a permutational mechanism for user identification and authentication.

6.1.1 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 authorized 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 authorized 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 authorized administrator performing the operation in each related log.

The logs are only accessible through the Web-Based administrative interface, in which only authenticated administrators are authorized to 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 authorized 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 authorized 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.

6.1.2 Cryptographic support

Secure Access provides an encrypted path between users and the TOE. Users connect to the TOE using a secure connection using TDES 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_COP.1: Triple Data Encryption Standard (TDES) as specified in FIPS PUB 46-2 algorithms are used to support encrypted communications between users and Secure Access.
- 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.

6.1.3 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 rue 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.

6.1.4 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 security function satisfies the explicit strength of function claim of SOF-medium which is supported by FIA_SOS.1, FIA_UAU.1 and FIA_UID.1.

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.

6.1.5 Security Management

Secure Access provides security management functions via a browser interface. The authorized 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 authorized administrator:
  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[6], modify, and view[7] 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.3: The TOE allows restrictive access by default but the authorized administrator can assign more restrictive permissions.
- FMT_SAE.1: The TOE allows the authorized administrator 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[8], modify, and view[9] 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.

6.1.6 Protection of the TSF

The Secure Access appliance is a hardened appliance that uses an optimized Linux kernel and additional server software. The system is designed to withstand attacks on the machine and attacks on data that pass though the appliance. The appliance protects against attacks on the machine by running only those services that are required to fulfill its mission and ensuring that those services have undergone careful scrutiny during the development process. Secure Access appliances do not run general-purpose user and application services, so they are not open to attack on those services. All user requests are subject to the identification and authentication and the information flow policies rules before any access is granted.

---

[6] The deletion of user attributes defined within FIA_ATD.1 is collectively performed through the deletion of the user account containing the attributes. Similarly, the creation of such attributes is performed through the creation of a user account with the exception for the association to a role, which is performed after user account creation.
[7] While an administrator can view a user's identity and role association, it is not possible to view a user's password.
[8] The deletion of user attributes defined within FIA_ATD.1 is collectively performed through the deletion of the user account containing the attributes. Similarly, the creation of such attributes is performed through the creation of a user account with the exception for the association to a role, which is performed after user account creation.
[9] While an administrator can view a user's identity and role association, it is not possible to view a user's password.

Process isolation is maintained in several ways. Each Secure Access appliance is completely self-contained. The hardware and firmware provided by appliances provide all the services necessary to implement the TOE. There are no external interfaces into the TOE other than the physical ports provided. No general programming interface is provided and no untrusted software runs on the appliance.

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 five 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_RVM.1: All users are subject to TOE security policies before any user's actions are permitted.
- FPT_SEP.1: The TOE maintains a domain for its own execution by not executing untrusting software and limiting its interfaces.
- FPT_STM.1: The TOE generates a reliable timestamp for its own use.
- FTA_SSL.1: The TOE protects existing encrypted sessions from becoming compromised by enforcing a session timeout after a session has been idle for more than five minutes or after a maximum session lifetime of 60 minutes has been reached, whichever comes first.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Juniper Networks ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Juniper Networks performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation.

These activities and their related configuration items are documented in:

- Juniper Networks Secure Access family 5.1R2 Configuration Management System

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Juniper Networks provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Juniper Networks' delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Juniper Networks also provides documentation that describes the steps necessary to install Secure Access in accordance with the evaluated configuration.

These activities are documented in:

- Juniper Networks Secure Access family 5.1R2 Delivery Guide
- Juniper Networks Secure Access family 5.1R2 Evaluated Configuration Guide

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Juniper Networks has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- Juniper Networks Secure Access family 5.1R2 Functional Specification
- Juniper Networks Secure Access family 5.1R2 High-level Design
- Juniper Networks Secure Access family 5.1R2 Correspondence Analysis

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Juniper Networks provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Juniper Networks NetScreen-SA 1000-6000, NetScreen Secure Access FIPS, Administration Guide, Release 5.1
- Juniper Networks Secure Access Online User Help[10]

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- Juniper Networks Secure Access family 5.1R2 Test Plan, Procedures, and Results

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

Juniper Networks has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

Juniper Networks performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Juniper Networks Secure Access family 5.1R2 Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

[10] The Juniper Networks Secure Access Online User Help consists of the user help dialogs available from within Secure Access's Administrator Console and End-User Interface.

7 Protection Profile Claims

There is no Protection Profile claim in this Security Target.

8 Rationale

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

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

8.1 Security Objectives Rationale

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	T.NOAUTH	T.REPLAY	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T. AUDFUL	T.TUSAGE	A.PHYSEC	A.LOWEXP	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.DIRECT	A.REMACC
O.IDAUTH	X																
O.MEDIAT			X	X													
O.SECSTA	X						X										
O.ENCRYP	X				X												
O.SELPRO							X	X									
O.AUDREC						X											
O.ACCOUN						X											
O.SECFUN	X							X									
O.LIMEXT	X																
O.SINUSE		X															
O.GUIDAN									X								
O. ADMTRA									X								
O.PHYSEC										X							
O.LOWEXP											X						
O.GENPUR												X					
O.PUBLIC													X				
O.NOEVIL														X			
O.SINGEN															X		
O.DIRECT																X	
O.REMACC																	X

Table 4 Environment to Objective Correspondence

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.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.
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.SECSTA	This security objective ensures that no information is comprised by the TOE upon startup or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.
O.ENCRYP	This security objective is necessary to counter the threats: T.NOAUTH and T.PROCOM by requiring that an administrator, read-only administrator, and user admin use encryption when performing administrative functions on the TOE remotely.
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.
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.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.SECFUN	This security objective is necessary to counter the threats: T.NOAUTH and 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.LIMEXT	This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an administrator to control and limit access to TOE security functions.
O.PHYSEC	The TOE is physically secure.
O.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
O.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.
O.PUBLIC	The TOE does not host public data.
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

O.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

O.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.

O.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training in the correct configuration, installation and usage of the TOE.

O.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

8.2 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FAU_GEN.1						X	X		
FAU_SAR.1						X			
FAU_STG.1					X			X	
FAU_STG.3					X			X	
FCS_COP.1				X					
FDP_IFC.1		X							
FDP_IFF.1		X							
FDP_RIP.1		X							
FIA_ATD.1	X								
FIA_SOS.1	X								
FIA_UAU.1	X								
FIA_UID.1	X						X		
FMT_MOF.1			X					X	X
FMT_MSA.3		X	X					X	
FMT_SAE.1								X	
FMT_SMF.1								X	
FMT_SMR.1								X	
FPT_RVM.1					X				
FPT_SEP.1					X				
FPT_STM.1						X			
FTA_SSL.3					X				
FTP_TRP.1				X					

Table 5 Objective to Requirement Correspondence

FAU_GEN.1 Audit data generation

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 Audit review

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 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized 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 Prevention of audit data loss

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_COP.1 Cryptographic operation

This component ensures that if when all users and administrators communicate with the TOE remotely from an internal or external network that DES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FDP_IFC.1 Subset information flow control

This component identifies the entities involved in the AUTHENTICATED USER information flow control 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 Simple security attributes

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 Subset residual information protection

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 User attribute definition

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.

FIA_SOS.1 Verification of secrets

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.

FMT_MOF.1 Management of security functions behavior

This component was chosen s in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FMT_MSA.3 Static attribute initialization

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.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_SAE.1 Time-limited authorization

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 Specification of management functions

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 Security roles

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_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked and succeed before each function within the TSC is allowed to proceed. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

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.

FTA_SSL.3 TSF-initiated termination

This component protects the TOE's communication path by terminating sessions idled for longer than 5 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 Trusted Path

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.

8.2.1 Strength of Function Claims Justification

Secure Access is targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a moderate attack potential. As such, minimum and explicit strength of function claims of 'SOF-medium' is appropriate for the intended environment. Note that the only applicable mechanisms (i.e., those that are probabilistic or permutational) are related to identification and authentication (FIA_SOS.1).

8.3 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

8.4 Requirement Dependency Rationale

The following table represents an analysis of the dependencies of the security functional requirements (SFRs) in this security target. The first column identifies all of the SFRs in this security target. The second column identifies the minimum dependencies defined in the Common Criteria v2.2. The third column identifies the actual requirements in this security target that correspond to the identified dependencies. There are two instances where the dependencies have not been met. See below for the rationale as to why the dependencies were not met.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	**Not included**
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3
FDP_RIP.1	none	none
FIA_ATD.1	none	none
FIA_SOS.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 and FPT_STM.1	FMT_SMR.1 and FPT_STM.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
FTP_TRP.1	none	none
FTA_SSL.3	none	none

Table 6 Requirement Dependencies

Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes.

Cryptographic modules are designed to meet the FIPS PUB 140-1standard. Per design, the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-1 compliant. For more information, refer to sections 4.8.1 and 4.8.5 of FIPS PUB 140-1.

8.5 Explicitly Stated Requirements Rationale

This ST does not contain any explicitly stated requirements.

8.6 TOE Summary Specification Rationale

This section provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 7 demonstrates the relationship between security requirements and security functions. Table 8 provides rationale explaining how the security functions satisfy the security requirements they may map to.

	Security Audit	**Cryptographic support**	**User data protection**	**Identification and Authentication**	**Security Management**	**Protection of the TSF**
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_STG.1	X					
FAU_STG.3	X					
FCS_COP.1		X				
FDP_IFC.1			X			
FDP_IFF.1			X			
FDP_RIP.1			X			
FIA_ATD.1				X		
FIA_SOS.1				X		
FIA_UAU.1				X		
FIA_UID.1				X		
FMT_MOF.1					X	
FMT_MSA.3					X	
FMT_SAE.1					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_RVM.1						X
FPT_SEP.1						X
FPT_STM.1						X
FTP_TRP.1		X				
FTA_SSL.3						X

Table 7 Security Functions vs. Requirements Mapping

Security Functions	SFRs	Rationale
Security Audit	FAU_GEN.1 FAU_SAR.1 FAU_STG.1 FAU_STG.3	The TOE implements audit data generation, review, and storage protection capabilities for audit data generated by SA. These events include modifications to the group of users that are part of a role, all use of the user identification mechanism, any use of the authentication mechanism, all decisions on requests for information flow with the exception for permitted access to a Windows file resource, changes to the time, start-up and shutdown of the TOE, creation, deletion, and modification of the information flow policies and user attributes, enabling and disabling external IT entities from communicating to the TOE, and archiving and clearing the audit trail.
Cryptographic support	FCS_COP.1 FTP_TRP.1	The TOE implements encryption capabilities for protecting the communication channel to users of the TOE. The TOE implements the encryption capabilities using Triple Data Encryption Standard (TDES) as specified in FIPS PUB 46-2 and implementing any mode of operation specified in FIPS PUB 81.
User data protection	FDP_IFC.1 FDP_IFF.1 FDP_RIP.1	The TOE implements user data protection by enforcing information flow control rules on all users accessing the TOE to control which resources may be accessed by individual users. The TOE also implements user data protection by ensuring that no previous content of a prior information flow is made available to other users of the TOE.
Identification and Authentication	FIA_ATD.1 FIA_SOS.1	The TOE implements identification & authentication capabilities for local authentication to the TOE using a password, which is verified to meet specific password strength. The TOE stores the user identity, user name, user roles, and password for each registered user of the TOE.
Security Management	FMT_MOF.1 FMT_MSA.3 FMT_SAE.1 FMT_SMF.1 FMT_SMR.1	The TOE implements security management capabilities for user management, role management, information flow policy management, audit management, and system start-up and shutdown of the TOE. The TOE also provides restrictive default values for information flow policy rules pertaining to individual users. However, the TOE provides the administrator of the TOE with the capability to override the default upon rule creation.
Protection of the TSF	FPT_RVM.1 FPT_SEP.1 FPT_STM.1 FTA_SSL.3	The TOE implements protection of the TSF by ensuring that no general-purpose user and application services can be installed on the TOE, providing a reliable time stamping mechanism for the audit records generated by the TOE, and protecting the TOE's communication channel by terminating sessions that are idled or have reached a maximum lifetime.

Table 8: Rationale for Security Functions Satisfying SFRs

8.7 PP Claims Rationale

See Section 7, Protection Profile Claims.