Cisco ASR9K with CRS-1/3, v4.1.1 Security Target

Version 1.0
November 1, 2011

Prepared for:
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive
Columbia, MD 21046

Table of Contents

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 is Cisco Aggregation Services Router (ASR) 9000 series, and the Carrier Routing System (CRS) routers CRS-1 and CRS-3 provided by Cisco Systems, Inc. The TOE is a family of Cisco high-capacity routers. The IOS XR, version 4.1.1 operating system code is shared across this family of routers.

The Security Target contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the assumptions and threats that define the security problem to be addressed by the TOE And its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment intended to counter the threats and satisfy the assumptions in the Security Problem Definition
- IT Security Requirements (Section 5)—presents a set of security functional requirements to be met by the TOE. The IT security requirements also provide a set of security assurance requirements that are to be satisfied by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the security functional requirements
- Protection Profile Claims (Section 7)—presents any protection profile claims
- Rationale (Section 8)—provides mappings and rationale for the security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Cisco ASR9K with CRS-1/3, v4.1.1 Security Target

ST Version – Version 1.0

ST Date – November 1, 2011

TOE Identification – Cisco Aggregation Services Router (ASR) 9000 series, with IOS XR operating system version 4.1.1 plus the following SMUs: asr9k-p-4.1.1.CSCtq56564, asr9k-p-4.1.1.CSCtr86240, and asr9k-p-4.1.1.CSCtq59879, and the Carrier Routing System (CRS) routers CRS-1 and CRS-3, with IOS XR operating system version 4.1.1 plus the following SMUs: hfr-px-4.1.1.CSCtq21686.pie, hfr-px-4.1.1.CSCtq59879.pie, hfr-px-4.1.1.CSCtr70418.pie, hfr-px-4.1.1.CSCtq16133.pie, hfr-px-4.1.1.CSCtr16132.pie

TOE Developer – Cisco Systems, Inc.

Evaluation Sponsor – Cisco Systems, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version v3.1 revision 3, July 2009

1.2 Conformance Claims

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

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version v3.1 revision 3, July 2009
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version v3.1 revision 3, July 2009

- Part 3 Conformant

- This ST and the TOE it describes are conformant to the following package:
  - EAL3 Augmented (ALC_FLR.2).

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements—Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parenthesis placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, 1 and 2.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Extended Requirements (i.e., those not found in Part 2 of the CC) are identified with "(EXT)" following the identification of the new functional class/name and the associated family descriptor. Example: (FPT_HA_(EXT).1 High Availability)
- Other sections of the ST—Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Abbreviations

Abbreviation	Definition
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
API	Application Programming Interface
ASR	Aggregation Services Router
CC	Common Criteria
CCEVS	CC Evaluation and Validation Scheme
CLI	Command Line Interface
CRS	Carrier Routing System
FCC	Fabric-Card Chassis
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTP	Hyper-text Transfer Protocol
HTTPS	Secure HTTP
IP	Internet Protocol
LCC	Line-Card Chassis
MPLS	Multiprotocol Label Switching
MPP	Management Plane Protection
OS	Operating System
POS	Packet over SONET/SDH
RADIUS	Remote Authentication Dial in User Service

Abbreviation	Definition
RP	Route Processor
RSP	Route Switch Processor
SFR	Security Functional Requirement
SMU	Service Module Upgrade
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SPA	Shared Port Adapter
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCAM	Ternary Content Addressable Memory
TCP	Transmission Control Protocol
TOE	Target of Evaluation
WAN	Wide Area Network
XML	Extensible Markup Language

2. TOE Description

The Target of Evaluation (TOE) is the Cisco ASR9K series , with IOS XR operating system version 4.1.1 plus the following SMUs: asr9k-p-4.1.1.CSCtq56564, asr9k-p-4.1.1.CSCtr86240, and asr9k-p-4.1.1.CSCtq59879, and CRS series with IOS XR Operating System Version 4.1.1 plus the following SMUs: hfr-px-4.1.1.CSCtq21686.pie, hfr-px-4.1.1.CSCtq59879.pie, hfr-px-4.1.1.CSCtr70418.pie, hfr-px-4.1.1.CSCtq16133.pie, hfr-px-4.1.1.CSCtr16132.pie. The TOE may also be identified as CRS-1/3, CRS, CRS-1, CRS-3, ASR9K, or ASR9K with CRS-1/3 throughout this document. The software may also be referred to simply as version 4.1.1 in this and other evaluation documentation.

2.1 TOE Overview

The TOE is a purpose-built, wide-area network (WAN) routing platform that provides basic security functionality including network Access Control Lists, administrative security, and firewall functionality. The TOE includes a number of chassis options: the ASR 9006 and ASR 9010, the CRS-1 4-slot, CRS-1 8-slot, and CRS-1 16-slot single shelf options, multiple shelf/chassis options of the CRS-1 16-slot, as well as upgraded switching fabric (CRS-3) models including CRS-3 4-slot, CRS-3 8-slot, CRS-3 16-slot single shelf options and multiple shelf/chassis options of the CRS-3 16-slot.

Each physical variation of the TOE features redundant routing engines (Route Processors or Route Switch Processors) as well as capability for highly-redundant power supplies and additional reliability features. These features provide High-Availability failover functionality. As noted above the TOE also supports firewall capabilities such as allowing network traffic to be monitored based on source and destination address as well as transport layer protocol defined in ACLs (Access Control Lists). The ASR 9000 Series Router is designed to provide the necessary feature set for routing of very high-speed network traffic at or near the edge of a service provider network, in a physically dense form factor with additional capability for upgraded speeds (100Gbps per port) in future without requiring a change to the chassis or switching fabric. The CRS series routers are designed to operate closer to the backbone or core of a major carrier or service provider, in an environment where much of the traffic is separated through MPLS (Multiprotocol Label Switching) or other techniques, and therefore provides fewer functions that are directly related to firewalling of traffic and more functions related to routing/switching the traffic at the very highest possible speed. As noted above, both the ASR9000 series and the CRS series provide security-relevant functionality to protect the router itself, to keep the control plane separate from the data plane, and to ensure that administrative interfaces are protected. More details of these functions are provided in the TOE Architecture (MPP) and in the TOE Summary Specification sections within this document.

The TOE provides capabilities to manage its routing functions, and controls access to those capabilities through the use of administrative roles with varying security management authorizations. All administrative users of the TOE are required to be identified and authenticated before accessing the TOE's management capabilities, and administrative actions are audited. Additionally, the TOE provides cryptographic capabilities to protect remote administrator sessions and information transmitted to remote authorized IT entities. These functions are described in more detail in the TOE Summary Specification within this document.

2.2 TOE Architecture

The TOE consists of the ASR 9000 Series Routers (ASR9K), and the CRS-1 and CRS-3 routers, each containing the IOS XR V4.1.1 Operating System and a primary command line interface (CLI). Alternate administrative interfaces include SNMPv3 (which is primarily used for monitoring but does provide a limited ability to administer the router and change configuration) and an Application Programming Interface (API) that allows complex router configurations to be added or changed using XML-formatted text in place of a series of individual CLI commands.

Route Processors (RPs) within CRS routers and Route Switch Processors (RSPs) within the ASR9K routers provide the advanced packet routing capabilities. The processors provide the monitoring, managing, and configuring services for the TOE itself. The CLI is provided, and TOE administration is performed, within the processors. In addition the RPs and RSPs negotiate and maintain encryption methods, and encryption keys between the TOE and external IT entities.

Shared Port Adapters (SPAs) provide the physical interfaces for TOE connectivity to the connected network including copper, channelized, POS, and Ethernet.

Outside the TOE physical boundaries but inside the relevant IT environment, the TOE will generally require one or more of an SSH client, an SNMPv3 engine/server, and/or a suitable Operations Support System (OSS) that provides secure XML management using the Cisco XML API, in order to support administration of the ASR9000 series or CRS series routers. In addition, an external RADIUS or TACACS+ authentication server may be used to provide authentication services to administrative users of the TOE.

The Management Plane Protection (MPP) feature in Cisco IOS XR software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows an administrator to designate one or more router interfaces as management interfaces. Once a management interface is configured and MPP is enabled, management traffic may only enter the device through this interface. The management interface is restricted to authorized administrators and provides the ability to manage the security functions and users of the TOE. The pre-defined management roles can be augmented with additional fine-grained defined roles to provide role separation.

2.2.1 Physical Scope – ASR 9000 Series (ASR9K) Routers

The ASR9K Series consists of two (2) chassis options, the Cisco ASR 9000 Series 6-Slot Chassis (ASR-9006) with 4 line cards and the Cisco ASR 9000 Series 10-Slot Chassis (ASR-9010) with 8 line cards. Both contain two slots dedicated for dual redundant Route Switch Processors (RSPs), modular fans, and AC or DC power supplies. Each Chassis contain a minimum of one RSP, nominally two per chassis. The RSPs provide routing engine as well as switching fabric with active non-blocking mode for redundant RSPs.

The following Ethernet modules are available for plug-in to either chassis:

- 40-port Gigabit Ethernet,
- 4-port 10GBps Ethernet,
- 8-port 10Gbps Ethernet line cards, and
- 2-port 10 Gigabit Ethernet + 20-port Gigabit Ethernet.

Each of the line card types is available in three “scale types” (High Queue, Medium Queue, and Low Queue) supporting differing numbers of simultaneous packet queues and related functionality.

A complete list of Ethernet line card variants is as follows:

- A9K-40GE-L
- A9K-40GE-B
- A9K-40GE-E
- A9K-4T-L
- A9K-4T-B
- A9K-4T-E
- A9K-8T/4-L
- A9K-8T/4-B
- A9K-8T/4-E
- A9K-2T20GE-L
- A9K-2T20GE-B
- A9K-2T20GE-E
- A9K-8T-L
- A9K-8T-B
- A9K-8T-E
- A9K-16/8T-B

Additionally, there is support for non-Ethernet interfaces in the Shared Port Adapter (SPA) form factor that is common to other Cisco routers. These SPAs are installed into the SPA Interface Processor line card A9K-SIP-700.

2.2.2 Physical Scope – CRS-1 Series Routers

There are two CRS-1 Series form factors: LCC and FCC.

The CRS-1 Series Router, LCC consists of three (3) chassis options: the Cisco CRS-1 4-slot chassis, the Cisco CRS-1 8-slot chassis, and the Cisco CRS-1 16-slot chassis.

Each CRS-1 16-Slot Line-Card Chassis includes:

- Two route processors (CRS-16-RP)
- Two CRS-1 16 fan controllers
- Eight CRS-1 16 fabric cards
- Two Power Shelves (either DC, AC type Wye, AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

Optional items include:

- 16 CRS-1 line cards
- 16 CRS-1 PLIMs.

Supported line cards for CRS-1 comprise:

- 1-port OC-768c/STM-256c packet over Synchronous Optical Network (POS) - 1OC768-POS-SR
- 1-port OC-768 DPSK+ (C-band) DWDM PLIM - 1OC768-DPSK/C 8-port 10 Gigabit Ethernet - 8-10GBE or 8-10GBE-WL-XFP
- 4-port 10 Gigabit Ethernet - 4-10GBE-WL-XFP
- CRS1-SIP-800 Carrier Card - CRS1-SIP-800
- 4-Port OC-3/STM-1 POS SPA
- 8-Port 1 Gigabit Ethernet SPA
- 1-port OC-768c/STM-256c Tunable WDMPOS
- 4-port 10GE Tunable WDMPHY
- 20-port 1 Gigabit Ethernet Flexible interface - 20-1GE-FLEX
- 1-port 100 Gigabit Ethernet - 1X100GBE
- 2-port.10 Gigabit Ethernet WAN/LAN Flexible - 2-10GE-WL-FLEX
- 14-port 10 Gigabit Ethernet LAN/WAN - 14X10GBE-WL-XFP
- 20-port 10 Gigabit Ethernet LAN/WAN - 20X10GBE-WL-XFP

The CRS-1 Series Router, FCC form factor, consists of one (1) chassis option: the Cisco CRS-1 24-Slot FCC. The Cisco CRS-1 24-Slot FCC is part of the CRS-1 16-slot multi-chassis system and includes:

- Two Cisco CRS-1 fan controllers (part number CRS-FCC-SC-22GE)
- Eight Cisco CRS-1 S2 fabric cards (part number CRS-FCC-SFC)
- Two power shelves (DC, AC type Wye, or AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

2.2.3 Physical Scope – CRS-3 Routers

The CRS-3 routers are physically identical to the CRS-1 routers other than the revised switching fabric. The TOE physical boundaries are the same between CRS-1 and CRS-3, but all the part numbers/nomenclature are different due to the improved switching fabric—therefore the CRS-1 and CRS-3 routers have been described separately.

There are two CRS-3 Series form factors: LCC and FCC.

The CRS-3 Series Router, LCC consists of three (3) chassis options: the Cisco CRS-3 4-slot chassis, the Cisco CRS-3 8-slot chassis, and the Cisco CRS-3 16-slot chassis.

Each Cisco CRS-3 16-slot line card chassis includes:

- Two route processors (CRS-16-RP)
- Two Cisco CRS-1 16 slot system fan controllers
- Eight Cisco CRS-3 16 slot system fabric cards
- Two power shelves (either DC, AC type Wye, or AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

Optional items include:

- 16 Cisco CRS-1 line cards or CRS-3 line cards
- 16 Cisco CRS-1 PLIMs or CRS-3 PLIMs.

Supported line cards for CRS-3 under IOS XR v4.1.1 are:

- 1-port OC-768c/STM-256c packet over SONET (PoS) - 1OC768-POS-SR
- 1-port OC-768 DPSK+ (C-band) DWDM PLIM - 1OC768-DPSK/C
- 8-port 10 Gigabit Ethernet (GE) - 8-10GBE or 8-10GBE-WL-XFP
- 4-port 10 GE - 4-10GBE-WL-XFP
- 1-port OC-768c/STM-256c tunable WDMPoS
- 4-port 10GE tunable WDMPHY
- 14-port 10GE LAN/WAN PHY - 14X10GBE-WL-XFP
- 20-port 10GE LAN/WAN PHY - 20X10GBE-WL-XFP
- 1-port 100GE - 1X100GBE
- Cisco CRS-1-SIP-800 Carrier Card - CRS1-SIP-800
- 2- and 4-port OC-3c/STM-1c PoS shared port adapters (SPAs)
- 1-, 2-, and 4-port OC-48c/STM-16c PoS/RPR SPAs
- 1-port OC-192c/STM-64c PoS/RPR SPA
- 1-port 10GE SPA
- 2-port and 4-port Clear Channel T3/E3 SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 PoS SPAs
- 2-port, 5-port, 8-port, and 10-port GE SPAs
- 1-port 10GE LAN/WAN-PHY SPA
- 20-port GE Flexible Interface Module - 20-1GE-FLEX
- 2-port 10GE WAN/LAN-PHY flexible interface module - 2-10GE-WL-FLEX .

The CRS-3 Series Router, FCC consists of one (1) chassis option: the Cisco CRS-3 24-Slot FCC. The Cisco CRS-3 24-Slot FCC is part of the CRS-3 16-slot multi-chassis system and includes:

- Two Cisco CRS-3 fan controllers (part number CRS3-FCC-SC-22GE)
- Eight Cisco CRS-3 S2 fabric cards (part number CRS3-FCC-SFC)
- Two power shelves (DC, AC type Wye, or AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

2.2.4 Logical Boundaries

This section identifies the security functions that are provided by the IOS XR family of routers (ASR9K and CRS-1/3 Routers with IOS XR v4.1.1). The logical boundaries of the TOE include the security functions of the TOE interfaces. The TOE logically supports the following security functions:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- User Data Protection
- Trusted Path/Channel
- Protection of the TSF
- TOE Access.

2.2.4.1 Security Audit

The TOE can audit events related to cryptographic functionality, information flow control enforcement, identification and authentication, and administrative actions. The IOS generates an audit record for each auditable event. Administrators can search, view and manage the set of auditable events.

2.2.4.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality, including AES, Triple DES and DSA, to support SSHv2, SNMPv3, and SSL. This cryptography is stated by the manufacturer to be conformant to the applicable FIPS publications; however, neither the algorithm implementations nor the embodiment have been formally validated[1].

2.2.4.3 Identification and Authentication

The TOE provides authentication services for administrative users wishing to connect to the TOE's secure CLI administrative interface. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. In addition, the TOE supports local and remote identification and authentication of TOE users. Unsuccessful authentication attempts can be limited based on authorized administrator configuration.

2.2.4.4 Security Management

The Management Plane Protection (MPP) feature in Cisco IOS XR software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows an administrator to designate one or more router interfaces as management interfaces. Once a management interface is configured and MPP is enabled, management traffic may only enter the device through this interface. The management interface is restricted to authorized administrators and provides the ability to manage the security functions and users of the TOE. The pre-defined management roles can be augmented with additional fine-grained defined roles to provide role separation.

2.2.4.5 User Data Protection

The TOE enforces the following information flow control policies:

- Unauthenticated TOE services—the TOE mediates all information flows to and from the TOE itself. The TOE has the ability to permit or deny information flows based on the characteristics of the information flow.
- Unauthenticated information flow—the TOE mediates all information flows through the TOE for unauthenticated information flows.

[1] For CRS, all cryptography is embodied within software modules. For ASR9000, the embodiment may include both software and hardware cryptographic modules. FIPS 140 validation has not been obtained for any embodiment.

2.2.4.6 Trusted Path/Channel

The TOE establishes a trusted path between itself and the remote management station used by the administrators to manage the TOE. This Trusted path is secured using an SSHv2[2], SSL, or SNMPv3 secure connection.

2.2.4.7 Protection of the TSF

The TOE is capable of preserving a secure state when software or hardware failures occur. The TOE provides manual and automatic recovery mechanisms. In addition, the TOE protects all TSF data from unauthorized modification and disclosure during transmission.

The TOE provides hardware failover for hardware or software faults within the TSF for configurations that include dual RPs or dual RSPs.

2.2.4.8 TOE Access

The TOE provides the capability for the TSF to determinate when there is user inactivity and terminates the session. A user will have to re-authenticate and start a new session. Advisory user interface banners can be configured.

2.3 TOE Documentation

Cisco offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

[2] IOS XR includes support for SSHv1 for backward compatibility, but for security reasons that support will be disabled in the TOE.

3. Security Problem Definition

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the TOE and the environment of the TOE counter
- Assumptions made about the operational environment and the intended method of use for the TOE.

3.1 Threats

The following are the threats to be addressed by the TOE in its assumed operational environment and method of use.

T.ADMIN_ERROR	An administrator may incorrectly configure or manage the TOE, resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's actions.
T.MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
T.SPOOFING	An entity may misrepresent itself as the TOE to obtain authentication data.
T.TSF_COMPROMISE	An attacker able to observe network communications between the TOE and remote administrators or remote IT entities may compromise TSF data.
T.UNACCOUNTABILITY	The authorized users of the TOE may not be held accountable for their actions within the TOE, resulting in unauthorized and undetected activities that compromise the TOE or the data it protects.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user sending data to or through the TOE may gain access to services for which they are not authorized according to the TOE security policy.
T.UNAUTHORIZED_USAGE	Through ignorance, a user may make inappropriate or unauthorized use of the TOE or use it in a fashion that is contrary to the site security policy.
T.UNAVAILABILITY	Hardware or software failures could cause the TOE to cease operating, resulting in its services being unavailable to authorized users.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations of the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

3.2 Assumptions

This section describes assumptions regarding the TOE's operational environment and intended method of use.

A.NO_GENERAL_PURPOSE	The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
A.EXTERNAL_AUTH	The TOE can utilize external RADIUS or TACACS+ authentication servers.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

O.AUDIT_GENERATION	The TOE shall provide the capability to detect, and create records of, security-relevant events associated with the operation of the TOE.
O.AUDIT_PROTECTION	The TOE shall protect audit information stored in the audit trail from unauthorized access.
O.AUDIT_REVIEW	The TOE shall provide administrators the capability to selectively view audit information stored in the audit trail.
O.AUTHENTICATION	The TOE shall be able to authenticate the claimed identities of administrative users and authorized remote IT entities.
O.CRYPTO_FUNCTIONS	The TOE shall provide cryptographic functions to support its security functions.
O.DISPLAY_BANNER	The TOE shall display an advisory warning regarding use of the TOE.
O.IDENTIFICATION	The TOE shall be able to identify all users of the TOE.
O.MANAGE	The TOE shall provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE shall mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.
O.PROTECTED_COMMS	The TOE shall be able to protect its communications with authorized remote IT entities from unauthorized disclosure and undetected modification.
O.SERVICE_CONTINUITY	The TOE shall provide capabilities to support continuity of TOE services in the event of a failure.
O.TOE_ACCESS	The TOE shall provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.TRUSTED_PATH	The TOE shall provide a means to ensure administrative users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.

4.2 Security Objectives for the Environment

OE.NO_GENERAL_PURPOSE	Those responsible for the TOE will ensure there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
OE.NO_TOE_BYPASS	Those responsible for the TOE will ensure information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.PHYSICAL	Those responsible for the TOE will ensure the operational environment provides physical security commensurate with the value of the TOE and the data it processes.

OE.EXTERNAL_AUTH	Those responsible for the TOE will ensure that the operational environment provides RADIUS and/or TACACS+ authentication servers to support external authentication options.

5. IT Security Requirements

5.1 Extended Components Definition

This Security Target contains one Security Functional Requirement (FPT_HA_(EXT).1) that is not drawn from existing CC part 2 Security Function Requirements.

5.1.1 Protection of the TSF (FPT)

Management: FPT_HA_(EXT.1)

There are no management activities foreseen.

Audit: FPT_HA_(EXT.1)

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Failure of the TSF.

5.1.1.1 High Availability (FPT_HA_(EXT.1))

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FPT_HA_(EXT).1.1 The TSF provides hardware failover for any single hardware or software fault within the TSF for any TOE configuration which includes dual RPs/RSPs.

The identification structure of the Security Functional Requirement is modeled after the Security Functional Requirements included in CC part 2. The identification structure includes the following:

A. Class – The extended SFR included in this ST is part of the FPT class of requirements. The FPT class of SFRs identifies TSF integrity functionality provided by the TOE. FPT_HA_(EXP).1 describes the high availability functionality provided by the TOE. High availability ensures that the integrity of the TOE and security functionality provided by the TOE are maintained even during specific failure events. This is integrity functionality and consistent with the FPT class of SFRs.

B. Family – The extended SFR included in this ST is part of a newly created SFR family, HA. This family was created to describe the high availability functionality provided by the TOE. There is not a family defined in the Common Criteria Part 2 to address the high availability functionality provided by the TOE. This is why the new family was created.

C. Component – This extended SFR has only one component in the family. This is why the component is identified as "1."

D. Element – This extended SFR comprises a single element specifying the conditions under which the TOE provides its hardware failover capability.

5.2 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 3, July 2009.

This ST includes extended requirements. The extended requirements can be identified by the use of the keyword "EXT" in the title.

Table 1: Security Functional Requirements (SFR)

Requirement Class	Requirement Component
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review

Requirement Class	Requirement Component
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FCS_CKM.1(1)	Cryptographic Key Generation
FCS_CKM.1(2)	Cryptographic Key Generation
FCS_CKM.1(3)	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1(1)	Cryptographic Operation
FCS_COP.1(2)	Cryptographic Operation
FCS_COP.1(3)	Cryptographic Operation
FCS_COP.1(4)	Cryptographic Operation
FCS_COP.1(5)	Cryptographic Operation
FDP_IFC.1(1)	Subset information flow control
FDP_IFC.1(2)	Subset information flow control
FDP_IFF.1(1)	Simple security attributes
FDP_IFF.1(2)	Simple security attributes
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FMT_MOF.1(1)	Management of security functions behavior – Security Audit
FMT_MOF.1(2)	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1(1)	Management of TSF data
FMT_MTD.1(2)	Management of TSF data
FMT_REV.1	Revocation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_RCV.2	Automated Recovery
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated termination
FTA_TAB.1	Default TOE access banners
FTA_TSE.1	TOE session establishment
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1(1)	Trusted path
FTP_TRP.1(2)	Trusted path
Explicitly Stated Security Functional Requirements	
FPT_HA_(EXT).1	High Availability

5.2.1 Security Audit (FAU)

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 [***basic***] level of audit; and

c) [**no specifically defined 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 (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 2**].

Table 2: Auditable Events Table

Requirement	Auditable Events	Audit Record Contents
FAU_GEN.1	None	
FAU_GEN.2	None	
FAU_SAR.1	Opening the audit trail and reading of information from the audit records.	The identity of the administrator performing the function.
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	The identity of the administrator performing the function.
FAU_SAR.3	The parameters used for the viewing.	The parameters used for the viewing.
FAU_STG.1	None	
FCS_CKM.1(1)	Success and failure of the activity and the object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	Identify the failed activity and the object and/or value.
FCS_CKM.1(2)	Success and failure of the activity and the object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	Identify the failed activity and the object and/or value.
FCS_CKM.4	Success and failure of the activity and the object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	Identify the failed activity and the object and/or value.
FCS_COP.1(1)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	Identify the mode of operation
FCS_COP.1(2)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	Identify the mode of operation
FCS_COP.1(3)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	Identify the mode of operation
FCS_COP.1(4)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	Identify the mode of operation

Requirement	Auditable Events	Audit Record Contents
FCS_COP.1(5)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	Identify the mode of operation
FDP_IFC.1(1)	None	
FDP_IFC.1(2)	None	
FDP_IFF.1(1)	All decisions on requests for information flow and the operation applied to each information flow permitted.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. Destination subject service identifier, if applicable. Identity of the interface on which the TOE received the packet. For denied information flows, the reason for denial.
FDP_IFF.1(2)	All decisions on requests for information flow and the operation applied to each information flow permitted.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. Destination subject service identifier, if applicable. Identity of the interface on which the TOE received the packet. For denied information flows, the reason for denial.
FIA_ATD.1	None	
FIA_UAU.1	All use of the authentication mechanism and successful and unsuccessful use of authentication mechanisms	Claimed identity of the user attempting identification.
FIA_UAU.5	The result of each activated mechanism together with the final decision.	Claimed identity of the user attempting to authenticate.
FIA_UID.2	All use of the user identification mechanism, including the user identity provided and unsuccessful use of the user identification mechanism, including the user identity provided	Claimed identity of the user using the identification mechanism.
FMT_MOF.1(1)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).

Requirement	Auditable Events	Audit Record Contents
FMT_MOF.1(2)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MSA.1	All modifications of the values of security attributes	The identity of the administrator performing the function, the function being performed and the security attributes being used to perform the function (if available).
FMT_MSA.3	All modifications of the initial values of security attribute.	The identity of the administrator performing the function, the function being performed, and the security attribute being used to perform the function (if available).
FMT_MTD.1(1)	All modifications to the values of TSF data (reliable timestamps)	The identity of the administrator performing the function, the function being performed and the values of TSF data being modified during the performance the function (if available).
FMT_MTD.1(2)	All modifications to the values of TSF data (information flow policy rule set)	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_REV.1	All attempts to revoke security attributes	List of security attributes that were attempted to be revoked. The identity of the administrator performing the function.
FMT_SMF.1	Use of the management functions	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_SMR.1	Modifications to the group of users that are part of a role	The identity of the administrator performing the function, the identity of the user and the role being modified.
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_HA_(EXT).1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_ITC.1	None	
FPT_ITI.1	None	
FPT_RCV.2	Type of failure or service discontinuity	Identify the failure, and that the TSF was able to recover to a secure state. If it is not possible to recover, enter maintenance mode.
FPT_STM.1	Changes to the time	The identity of the administrator performing the function

Requirement	Auditable Events	Audit Record Contents
FTA_TAB.1	None	
FTP_ITC.1	a) Failure of the trusted channel functions. b) Identification of the initiator and target of failed trusted channel functions. c) All attempted uses of the trusted channel functions. d) Identifier of the initiator and target of all trusted channel functions.	Indicated that the trusted channel failed and identification of the initiator and target of all trusted channels.
FTP_TRP.1(1) Application Note: While this requirement applies to SSH, SSL, and SNMP protocols, the log generation only occurs for SSH and SSL.	a) Failures of the trusted path functions. b) Identification of the user associated with all trusted path failures, if available. c) All attempted uses of the trusted path functions. d) Identification of the user associated with all trusted path invocations, if available.	Indicated that the trusted path failed and Identification of the claimed user identity.
FTP_TRP.1(2) Application Note: While this requirement applies to SSH, SSL, and SNMP protocols, the log generation only occurs for SSH and SSL.	a) Failures of the trusted path functions. b) Identification of the user associated with all trusted path failures, if available. c) All attempted uses of the trusted path functions. d) Identification of the user associated with all trusted path invocations, if available.	Indicated that the trusted channel failed and Identification of the claimed user identity.

FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**root-system, netadmin, sysadmin, operator, root-lr, and users assigned logging task ID**] with the capability to read [**all audit data**] from the audit records.

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

FAU_SAR.2 Restricted Audit Review

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

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches**] of audit data based on [

a) **user identity;**
b) **ip address;**
c) **ranges of date and time;**
d) **combinations of one or more of the following: date, time, user identitie, subject service identifier, or transport layer protocol;**
e) **rule identity; and**
f) **TOE network interfaces**].

Application Note: The timestamp of the events in the main syslog buffer on the TOE does not contain the year, so care must be taken during searches based on the date. The administrator must first examine the start and end of the syslog to ensure that the dates do not span a period greater than 12 months.

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 stored audit records in the audit trail.

5.2.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**DSA key generation algorithm**] and specified cryptographic key sizes [**1024 bits**] that meet the following: [**FIPS 186-3**].

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation algorithm**] and specified cryptographic key sizes [**1024, 2048 bits**] that meet the following: [**FIPS 186-3**].

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ANSI X9.31 Appendix A.2.4 PRNG**] and specified cryptographic key sizes [**128, 192, 256 bits for AES; 168 bits for 3DES**] that meet the following: [**ANSI X9.31**].

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 with zeroes**] that meets the following: [**none**].

FCS_COP.1 Cryptographic Operation

FCS_COP.1.1(1) The TSF shall perform [**symmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CBC, 3DES in CBC**] and cryptographic key sizes [**128, 192, 256 bits for AES; 168 bits for 3DES**] that meet the following: [**FIPS PUB 197 (AES); FIPS PUB 46-3 (3DES)**].

FCS_COP.1.1(2) The TSF shall perform [**cryptographic signature services**] in accordance with a specified cryptographic algorithm [**DSA or RSA**] and cryptographic key sizes [**1024 bits (DSA), 1024 or 2048 bits (RSA)**] that meet the following: [**FIPS PUB 186-3**].

FCS_COP.1.1(3) The TSF shall perform [**cryptographic key agreement services**] in accordance with a specified cryptographic algorithm [**Diffie-Hellman**] and cryptographic key sizes [**1024 bits, 2048 bits**] that meet the following: [**RFC 2631**].

FCS_COP.1.1(4) The TSF shall perform [**Secure Shell v2.0**] in accordance with ~~a~~ **the** specified cryptographic algorithm**s** [**AES or 3DES, SHA, DSA, Diffie-Hellman**] and cryptographic key sizes [**128, 192, and 256 bits (AES), 2048 bits (DSA), not applicable for SHA, and 2048 bits (Diffie-Hellman)**] that meet the following:[**AES (see FCS_COP.1(1)), DSA (see FCS_COP.1(2)),**

SHA, Diffie-Hellman (see FCS_COP.1(3)), and SSHv2.0 (Transport Layer -RFC 4253, User Authentication Layer – RFC 4252, Connection Layer – RFC 4255)].

FCS_COP.1.1(5) The TSF shall perform [**Secure Sockets Layer v3**] in accordance with ~~a~~ **the** specified cryptographic algorithm**s** [**AES, SHA, DSA or RSA**] and cryptographic key sizes [**128, 192, or 256 bits (AES), 1024 (DSA), 1024 or 2048 bits (RSA), and not applicable for SHA**] that meet the following:[**AES (see FCS_COP.1(1)), DSA and RSA (see FCS_COP.1(2)), SHA – FIPS 180-2**].

5.2.3 User Data Protection (FDP)

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1(1) The TSF shall enforce the [**UNAUTHENTICATED TOE SERVICES SFP**] on: [

a) subjects: source subject: TOE interface on which information is received, destination subject: the TOE;

b) information: network packets; and

c) operations: accept or reject network packet].

FDP_IFC.1.1(2) The TSF shall enforce the [**UNAUTHENTICATED INFORMATION FLOW SFP**] on: [

a) subjects: source subject: TOE interface on which information is received, destination subject: TOE interface to which information is destined;

b) information: network packets; and

c) operations:

- **pass information by opening a relay connection through the TSF on behalf of the source subject to the destination subject, and with the TSF ensuring the following conditions:**
  - **the connection from the source subject is from a valid peer network,**
  - **the new relay connection is established to the destination subject on a valid peer network**].

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1(1) The TSF shall enforce the [**UNAUTHENTICATED TOE SERVICES SFP**] based on the following types of subject and information security attributes[3]: [

a) Source subject security attributes:

- **set of source subject identifiers (IP address);**

b) Destination subject security attributes:

- **TOE's network identifier (IP address);**

c) Information security attributes:

- **presumed identity of source subject;**
- **identity of destination subject;**
- **protocol; and**
-
- **ICMP message type and code as specified in RFC 792].**

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

- **the presumed identity of the source subject is in the set of source subject identifiers;**
- **the identity of the destination subject is the TOE;**
- **the information security attributes match the attributes in an information flow control policy according to the following algorithm:**
  - **The TOE examines the packet security attributes (including, presumed identity of source subject (IP address), identity of destination subject (IP address), protocol, and compares the packet to the configured information flow policy rules,**

[3] The attributes combine to form an Access Control Entry (ACE), and a group of ACEs combine to form an Access Control Lists (ACL), as described in Section 6.1.3.

- **Each configured information policy is treated as an ordered list and the first rule that matches is the one the TSF acts on,**
- **The TOE accepts the network traffic if the first matching rule it encounters is an allow rule, and rejects the network traffic if either the first matching rule it encounters is a deny rule or it does not encounter any matching rules in the policy ruleset].**

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

- **The TOE shall allow source subjects to access TOE ICMP services without authenticating those source subjects; and**
- **The TOE shall allow the services specified immediately above to be enabled (become available to unauthenticated users) or disabled (become unavailable to unauthenticated users)**].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules [**no explicit authorization rules**].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [

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

FDP_IFF.1.1(2) The TSF shall enforce the [**UNAUTHENTICATED INFORMATION FLOW SFP**] based on the following types of subject and information security attributes[4]: [

a) Source subject security attributes:
- **set of source entity identifiers (IP address); and**

b) Destination subject security attributes:
- **Set of destination entity identifiers (IP address); and**

c) Information security attributes:
- **presumed identity of source entity;**
- **identity of destination entity;**
- **transport layer protocol;**
- **source entity service identifier;**
- **destination entity service identifier (e.g., TCP or User Datagram Protocol (UDP) destination port number)**].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **the presumed identity of the source entity is in the set of source entity identifiers;**
- **the identity of the destination entity is in the set of destination entity identifiers;**
- **the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by an administrator) according to the following algorithm:**
  - **Network traffic is received by the TOE on one of its interfaces,**
  - **The TOE examines the packet security attributes (including, presumed identity of source entity, identity of destination entity, transport layer protocol, source**

[4] The attributes combine to form an Access Control Entry (ACE), and a group of ACEs combine to form an Access Control Lists (ACL), as described in Section 6.1.3.

subject service identifier, destination subject service identifier (e.g., TCP or UDP destination port number) and compares the packet to the configured information flow policy rules,

- **Each configured information policy rule is treated as an ordered list and the first rule that matches is the one the TSF acts on,**

- **The TOE passes the network traffic if it meets a configured allow policy and does not meet a configured drop policy; and**
- **The selected information flow policy rule specifies that the information flow is to be permitted**].

FDP_IFF.1.3(2) The TSF shall enforce the: [

- **fragmentation rule:**
  - **prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets**].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules [**no explicit authorization rules**].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [

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

5.2.4 Identification and Authentication (FIA)

FIA_ATD.1 User Attribute Definition

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

- **User identifier**
- **Password**
- **User group (including task IDs and permissions).**

FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [**ICMP services**] on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide [**local and remote authentication mechanisms**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

- **If configured, RADIUS or TACACS+ authentication mechanism shall be used for authorized administrators to access the TOE. The TOE then accepts or rejects the authentication material based upon the response from the RADIUS or TACACS+ server before allowing any other TSF-mediated actions on behalf of that authorized administrator**

- **If RADUIS or TACACS+ is not configured or available, the TOE shall perform identification and authentication before allowing any other TSF-mediated actions on behalf of that authorized administrator**].

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.

5.2.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to [***determine the behaviour of, disable, enable, modify the behavior of***] the functions [**the audit functions defined in FAU_SAR.***] to [**root-system, sysadmin, netadmin, and administrators with logging task ID**].

FMT_MOF.1.1(2) The TSF shall restrict the ability to [***enable, disable***] the functions [**ICMP**] to [**root-system, root-lr, netadmin, sysadmin, administrators with acl task ID**].

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**UNAUTHENTICATED INFORMATION FLOW SFP, UNAUTHENTICATED TOE SERVICES SFP**] to restrict the ability to [***modify, delete***] the security attributes [**referenced in the indicated polices defined in FDP_IFC.* and FDP_IFF.***] to [**root-system, root-lr, netadmin, sysadmin, administrators with acl task ID**].

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [**UNAUTHENTICATED INFORMATION FLOW SFP, UNAUTHENTICATED TOE SERVICES 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 [**root-system, root-lr, netadmin, sysadmin, administrators with acl task ID**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***query, modify, delete, [set]***] the [**time and date used to form the time stamps in FPT_STM.1**] to [**root-system, root-lr, netadmin, sysadmin, authorized administrators with host-services task ID**].

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***query, modify, delete, [create]***] the [**information flow policy rules**] to [**root-system, root-lr, netadmin, sysadmin, administrators with acl task ID**].

FMT_REV.1 Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke [

- **for a user, their User group (including task IDs and permissions)**
- **for the information flow policy ruleset, an individual access control list**]

associated with the [***users, [information flow policy ruleset]***] under the control of the TSF to [**root-system, root-lr, netadmin, sysadmin, administrators with aaa task ID (user), administrators with acl task ID (information flow policy ruleset)**].

FMT_REV.1.2 The TSF shall enforce the rules: [

- **revocation of a user's role upon next login;**
- **revocation of an information flow policy ruleset upon next call to the flow policy security function**].

FMT_SMF.1 Specification of Management Functions

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

- **Management of user accounts**
- **Management of audit data and audit configurations**
- **Management of information flow SFP**
- **Management of security attributes used to enforce the SFP**
- **Management of time interval for session inactivity**
- **Configuration of the TOE access banner**
- **Management of the time and date used to form the time stamps in FPT_STM.1**]

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**operator, root-system, root-lr, sysadmin, netadmin, serviceadmin, administrators assigned the following task IDs: logging; acl; aaa; host-services; tty-access; crypto**].

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

5.2.6 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**all failures**].

FPT_ITC.1 Inter-TSF confidentiality during transmission

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

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [**immediately when TSF data is received by the TOE**].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [**disregard the information**] if modifications are detected.

FPT_RCV.2 Automated Recovery

FPT_RCV.2.1 When automated recovery from [**any hardware failure, any software failure**] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2 For [

- **Dual RP or RSP TOE configurations (ASR9000 series or CRS-1/-3)**
  - **Any single hardware failure on the active RP or RSP**
  - **Any single hardware failure on the standby RP or RSP**
  - **Any single software failure on the active RP or RSP**
  - **Any single software failure on the standby RP or RSP]**

the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_STM.1 Reliable time stamps

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

FPT_HA_(EXT).1 High Availability

FPT_HA_(EXT).1.1 The TSF provides hardware failover for any single hardware or software fault within the TSF for any TOE configuration which includes dual RPs/RSPs.

5.2.7 TOE Access (FTA)

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**administrator-configurable time interval of session inactivity**].

FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**remote location (IP address) and connecting network interface**].

5.2.8 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**all authentication functions delegated to a remote authentication server**].

FTP_TRP.1 Trusted path

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

FTP_TRP.1.2(1) The TSF shall permit [**authenticated administrator and authenticated users**] to initiate communication via the trusted path.

FTP_TRP.1.3(1) The TSF shall require the use of the trusted path for [***initial user authentication, [all remote administration actions]***].

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

FTP_TRP.1.2(2) The TSF shall permit [**authenticated administrator and authenticated users**] to initiate communication via the trusted path.

FTP_TRP.1.3(2) The TSF shall require the use of the trusted path for [***initial user authentication, [all remote administration actions]***].

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 3 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 3: EAL3 augmented with ALC_FLR.2 Assurance Components

Requirement Class	Requirement Component
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

Requirement Class	Requirement Component
ALC: Life-cycle support	ALC_CMC.3: Authorisation 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

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

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

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

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

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

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

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

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

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

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

5.3.1.2 Functional specification with complete summary (ADV_FSP.3)

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

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

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Architectural design (ADV_TDS.2)

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

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

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

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

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

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

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

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

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

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

5.3.2.2 Preparative Procedures (AGD_PRE.1)

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

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

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

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

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

5.3.3 Life-cycle Support (ALC)

5.3.3.1 Authorisation controls (ALC_CMC.3)

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.1C The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

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

5.3.3.2 Implementation representation CM coverage (ALC_CMS.3)

ALC_CMS.3.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

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

5.3.3.3 Delivery procedures (ALC_DEL.1)

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

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

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

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

5.3.3.4 Identification of security measures (ALC_DVS.1)

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

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

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

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

5.3.3.5 Flaw reporting procedures (ALC_FLR.2)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3.4 Tests (ATE)

5.3.4.1 Analysis of coverage (ATE_COV.2)

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

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

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

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

5.3.4.2 Testing: basic design (ATE_DPT.1)

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

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

5.3.4.3 Functional testing (ATE_FUN.1)

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, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test.

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

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

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

5.3.4.4 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 execute a sample of tests in the test documentation to verify the developer test results.

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

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability analysis (AVA_VAN.2)

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

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

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

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

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

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

6. TOE Summary Specification

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

6.1 TOE Security Functions

The TOE implements the following security functions that together satisfy the SFRs claimed in Section of this ST:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- User Data Protection
- Trusted Path/Channel
- Protection of the TSF
- TOE Access.

6.1.1 Security Audit

The TOE generates an audit record that is stored internally within the TOE whenever an auditable event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit function; audit searching; cryptography related events; events related to the enforcement of information flow policies; identification and authentication related events; and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the audit records stored in the audit trail internal to the TOE provides sufficient detail to identify the user with which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.

The audit record associated with each auditable event generated by the TOE is described in sufficient detail to allow an administrative user reviewing the audit log to identify which user the auditable event is associated with.

The audit trail is composed of both a local syslog store, accessed via the "show logging" command, and a CLI History file, accessed via the "show cli history detail" command.

The logging functionality on the TOE cannot be completely turned off. Each of the configured logging facilities can be individually turned off, except the CLI History file. Enabling and disabling all other logging facilities is captured in the CLI History file.

All security management commands associated with security audit security function require the administrator to have the `logging` Task ID (see Section 6.1.5, Security Management for details of how Task IDs are used to grant administrative privileges to users). The root-system, sysadmin, and netadmin predefined user group have Read/Write/Execute/Debug permissions for this Task ID. The root-lr and operator predefined user groups have Read access for this Task ID.

Administrators with Read/Write/Execute/Debug permissions for the `logging` Task ID can, through the CLI, perform the following operations associated with the security audit function:

1. View all of the audit events in the audit logs—these event records are presented in a manner in which the administrator can interpret the information
2. Search the audit records—the criteria by which audit records can be searched include: user identity; ip address; ranges of date and time; combinations of one or more of the following: date, time, user identity, subject service identifier, or transport layer protocol; Rule identity (the identifier in the syslog record that indicates the type of syslog record); or TOE network interfaces

3. Configure back-ups and manages audit data storage—the audit trail is normally configured to be circular, such that the oldest audit records are overwritten. The audit trail can be stored locally on the router and/or remotely with an interoperable syslog server. Although a remote syslog server may provide additional capabilities for sorting, searching, and audit reduction, such capabilities are outside the TOE. The administrator can configure the audit trail to be automatically backed up at a chosen frequency. The audit records can be saved by severity level and can be saved on local flash or hard drive
4. Delete the audit trail.

   Administrators with Read access for the `logging` Task ID can only perform parts 1 and 2 above.

Note that for SNMP there is no syslog generated upon detection of encryption failures and integrity issues. The packet is dropped without generation of a syslog event, but counters are kept of the failures that can be viewed with the "show snmp" command.

6.1.1.1 Security function summary

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

- FAU_GEN.1: The TSF generates audit events for the events defined and records the specified information in the audit log
- FAU_GEN.2: For audit events resulting from actions of identified users, the TSF is able to associate each auditable event with the identity of the user that caused the event
- FAU_SAR.1: The TSF provides authorized users with the capability to read all audit information from the audit records. The TSF provides the audit records in a manner suitable for the user to interpret the information
- FAU_SAR.2: The TSF prohibits all users read access to the audit records, except those users that have been granted explicit read-access (by being granted the `logging` Task ID)
- FAU_SAR.3: The TSF provides the ability to apply searches of audit data based on various attributes
- FAU_STG.1: The TSF protects the stored audit records in the audit trail from unauthorized deletion. The TSF prevents unauthorized modifications to the stored audit records in the audit trail.

6.1.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. This cryptography is stated by the manufacturer to be conformant to the applicable FIPS publications; however, neither the algorithm implementations nor the embodiment have been formally validated[5] The TOE provides cryptography to protect communications between itself and external authentication servers (using SSLv3) and in support of secure remote administration, which may use either SSHv2 for administration through a Command Line Interface (CLI) or SNMPv3 to administer the router using specific SNMP users (defined on the router) and MIBs. There is also a capability to administer certain router features using XML syntax over SSLv3 of SSHv2.

The TOE implements a pseudo-random number generator to support generation of DSA and RSA key-pairs, which is done in accordance with FIPS PUB 186-3. Keys are generated at the request of an administrator using the `crypto key generate` CLI command. The TOE also provides the administrator with a command to destroy RSA and DSA keys by overwriting them with 0's (`crypto key zeroize`).

In addition, the TOE automatically generates symmetric (AES or Triple DES) keys for encrypting and decrypting session data once an SSHv2 or SSL session has been established with the external IT entity. These keys are automatically destroyed by the TOE, by overwriting with 0's, when the session is terminated.

The following tables identify the cryptography provided by the TOE and its use.

[5] For CRS, all cryptography is embodied within software modules. For ASR9000, the embodiment may include both software and hardware cryptographic modules. FIPS 140 validation has not been obtained for any embodiment.

Table 4: SSHv2 Related Cryptography

Cryptographic Method	Use within SSHv2
SP 800-56 Key Exchange	Used in SSHv2 session establishment.
DSA Digital Signatures	Used in SSHv2 session establishment.
ANSI X9.31 PRNG	Used in SSHv2 session establishment.
SHS, hmac-md5	Used to provide SSHv2 traffic integrity verification.
AES	Used to encrypt SSHv2 session traffic.
3DES	Used to encrypt SSHv2 session traffic

Table 5: SSLv3 Related Cryptography

Cryptographic Method	Use within SSLv3
DSA or RSA Digital Signatures	Used in SSLv3 session establishment.
ANSI X9.31 PRNG	Used in SSLv3 session establishment.
SHS	Used to provide SSLv3 traffic integrity verification.
3DES	Used to encrypt SSLv3 session traffic.

Table 6: SNMPv3 Related Cryptography

Cryptographic Method	Use within SNMPv3
HMAC-MD5 or HMAC-SHA	Used for initial authentication (authNoPriv or authPriv mode)
AES	Used to encrypt SNMPv3 session traffic (authPriv mode only).
3DES	Used to encrypt SNMPv3 session traffic (authPriv mode only).

6.1.2.1 Security function summary

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

- FCS_CKM.1(1): The TOE generates asymmetric keys to support DSA cryptographic operations
- FCS_CKM.1(2): The TOE generates asymmetric keys to support RSA cryptographic operations
- FCS_CKM.1(3): The TOE generates symmetric keys to support AES and Triple DES cryptographic operations
- FCS_CKM.4: The TOE destroys cryptographic keys by overwriting them with zeroes
- FCS_COP.1(1): The TOE implements DSA (with 1024 or 2048 bit keys) to provide digital signature generation and verification services in support of SSH
- FCS_COP.1(2): The TOE implements AES and Triple DES to provide symmetric encryption and decryption services
- FCS_COP.1(3): The TOE implements Diffie-Hellman to provide cryptographic key agreement services
- FCS_COP.1(4): The TOE implements SSHv2 using the cryptographic capabilities specified in FCS_COP.1(1), FCS_COP.1(2) and FCS_COP.1(3)

- FCS_COP.1(5): The TOE implements SSLv3 using the cryptographic capabilities specified in FCS_COP.1(1), FCS_COP.1(2) and FCS_COP.1(3).

6.1.3 User data protection

The TOE enforces two information flow control policies—Unauthenticated TOE Services and Unauthenticated Information Flow.

Unauthenticated TOE Services

The TOE mediates all information flows to and from the TOE itself. The TOE has the ability to permit or deny information flows based on the characteristics of the information flow. By examining the information flows to the TOE itself, the TOE is able to provide ICMP services to requesting unauthenticated entities. All other TOE services are only available to authenticated entities.

Administrators, comprising **root-system**, **root-lr**, **netadmin, sysadmin,** and users assigned the `acl` Task ID (see Section 6.1.5, Security Management for details of how Task IDs are used to grant administrative privileges to users) are able to configure Unauthenticated TOE Service policies for network traffic requesting services provided by the TOE.

The policies used to control access to TOE services are implemented as Access Control Lists, comprising Access Control Entries (ACEs) that collectively define the network traffic profile. Each ACE includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

When network traffic is received by the TOE requesting TOE services (i.e., ICMP), the source of the traffic (IP address) and the attributes of the packet are compared against the policy. The TOE then accepts or rejects the traffic depending on the information flow policy for which the traffic meets.

The TOE tests the source or destination address or the protocol of each packet being filtered against the conditions in the access list, one condition (permit or deny statement) at a time. If a packet does not match an access list statement, the packet is then tested against the next statement in the list. If a packet and an access list statement match, the remaining statements in the list are skipped and the packet is accepted or rejected as specified in the matched statement. The first entry that the packet matches determines whether the software permits or denies the packet. That is, after the first match, no subsequent entries are considered. If the access list denies the address or protocol, the TOE discards the packet and returns an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP is configurable in the TOE software. If no conditions match, the TOE drops the packet because each access list ends with an unwritten or implicit deny statement. That is, if the packet has not been permitted or denied by the time it was tested against each statement, it is denied.

In the following instances, the TOE rejects the information flow:

- The TOE rejects requests for access or services where the source IP address of the network traffic is not included in the set of allowed source IP address;
- The TOE rejects requests for access or services where the source IP address of the network traffic is a broadcast address;
- The TOE rejects requests for access or services where the source IP address of the network traffic is a defined loopback address; and
- The TOE rejects requests for which the network traffic received by the TOE that specifies the route by which the traffic flows

Unauthenticated Information Flow

The TOE mediates all information flows through the TOE for unauthenticated information flows. The TOE provides the ability to classify all data flows into zones. Configurable allow or deny rule sets are applied to each information flow on a zone by zone basis. All security attributes are inspected based on the configurable rule set of the information flow. The TOE makes the decision to allow or deny unauthenticated information flows based on the configured information flow rule set. The TOE generates and maintains “state” information for all approved

connections mediated by the TOE. The "state" information is used to monitor the status of an approved connection and validate incoming packets received as part of an approved connection.

Authorized administrators, comprising **root-system**, **root-lr**, netadmin, sysadmin, and users assigned the `acl` Task ID, configure unauthenticated information flow policies for network traffic flowing through the TOE.

When network traffic is received the TOE, the TOE examines the attributes of the packet and compares the traffic to the configured information flow policies. The TOE finally allows or does not allow the traffic to flow depending on the information flow policy for which the traffic meets.

The policies used to control information flow are implemented as Access Control Lists, comprising Access Control Entries (ACEs) that collectively define the network traffic profile. This profile can then be referenced by TOE software features such as traffic filtering, priority or custom queueing, and dynamic access control. Each ACE includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

The TOE tests the source or destination address or the protocol of each packet being filtered against the conditions in the access list, one condition (permit or deny statement) at a time. If a packet does not match an access list statement, the packet is then tested against the next statement in the list. If a packet and an access list statement match, the remaining statements in the list are skipped and the packet is permitted or denied as specified in the matched statement. The first entry that the packet matches determines whether the software permits or denies the packet. That is, after the first match, no subsequent entries are considered. If the access list denies the address or protocol, the software discards the packet and returns an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP is configurable in the TOE software. If no conditions match, the software drops the packet because each access list ends with an unwritten or implicit deny statement. That is, if the packet has not been permitted or denied by the time it was tested against each statement, it is denied.

For messages received in fragments, the TOE also reassembles the packets using Virtual Fragment Reassembly. The TOE holds all fragments it receives until it receives a full message and assembles them. If the assembled message is permitted to flow, then the TOE passes the packet. The traffic is sent out as it was received, fragmented.

6.1.3.1 Security function summary

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

- FDP_IFC.1(1): The TSF shall enforce the UNAUTHENTICATED TOE SERVICES SFP on: subjects: source subject: TOE interface on which information is received, destination subject: the TOE; information: network packets; and operations: accept or reject network packet.
- FDP_IFC.1(2): The TSF shall enforce the UNAUTHENTICATED INFORMATION FLOW SFP on: subjects: source subject: TOE interface on which information is received, destination subject: TOE interface to which information is destined; information: network packets; and operations: pass information by opening a relay connection through the TSF on behalf of the source subject to the destination subject, and with the TSF ensuring the following conditions: the connection from the source subject is from a valid peer network, the new relay connection is established to the destination subject on a valid peer network.
- FDP_IFF.1(1): The TSF shall enforce the UNAUTHENTICATED TOE SERVICES SFP based on the defined types of subject and information security attributes: The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation based on the defined rules. The TSF shall enforce the defined flow control rules. The TSF shall explicitly deny an information flow based on the defined rules.
- FDP_IFF.1(2): The TSF shall enforce the UNAUTHENTICATED INFORMATION FLOW SFP based on the defined types of subject and information security attributes: The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation based on the defined rules. The TSF shall enforce the defined flow control rules. The TSF shall explicitly deny an information flow based on the defined rules.

6.1.4 Identification and Authentication

The TOE provides local authentication services for administrative users wishing to connect to the TOE's secure CLI administrative interface. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. The TOE also supports both RADIUS and TACACS+ servers for remote AAA, depending on customer requirements. If configured to use RADIUS or TACACS authentication mechanism then the RADIUS or TACACS server provides the TOE with either accept or reject information and the TOE enforces this decision. If RADIUS or TACACS is not configured or is unavailable, then the TOE performs identification and authentication. The administrator must provide a valid username and password in order for the TOE to successfully authenticate the administrator.

The TOE provides the ability for an authorized administrator to configure all TOE services through the TOE administrative CLI. When a TOE interface is configured and the "no shut" command is applied it responds to the "to us" pings but passing any other traffic requires configuring an appropriate route. Administrative access to the TOE is facilitated through the TOE provided CLI. The TOE mediates all actions through the CLI. Once a potential administrative user attempts to access the management functionality of the TOE through either a directly connected console or remotely through an SSHv2 connection, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative facilities of the TOE until an administrator is authenticated.

The TOE provides a basic set of pre-defined user roles and allows flexible definition of additional roles to meet customer needs. This is discussed further in Section 6.1.5.

The TOE maintains the following attributes for each administrative user of the TOE: user identity; user group (through which the user is associated with security management privileges); and password. These user attributes are also maintained on the remote authentication server if one is configured. The user name and password are used by the TOE to authenticate an administrator wishing to gain access to the TOE management functionality. Note that the TOE supports both RADIUS and TACACS+ servers for remote AAA, depending on customer requirements. The methodology for defining additional task groups on a remote server is to identify a task (or set of tasks) and specify them as an attribute of a user group in the external server. An example provided in Cisco documentation for creation of a user "igpadmin" that is a member of "igp-admin-group"and that can perform tasks related to OSPF routing (used as an interior gateway protocol, or IGP) with privileges as user group "operator", is

```
user = igpadmin{
       member = igp-admin-group
       opap = cleartext "cisco"
       service = exec {
       task = "rwxd:ospf,#operator"
       }
}
```

6.1.4.1 Security function summary

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

- FIA_ATD.1: The TSF maintains the following list of security attributes belonging to individual users: user identifier, user group, password
- FIA_UAU.1: The TSF can allow ICMP services on behalf of the user to be performed before the user is authenticated. The TSF requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user
- FIA_UAU.5: The TSF provides local and remote authentication mechanisms to support user authentication. The TSF authenticates any user's claimed identity according to the following rules: if configured, RADIUS or TACACS authentication mechanisms are used for authorized administrators to access the TOE. The TOE then accepts or rejects the authentication decision based on the response from the RADIUS or TACACS server, before allowing any other TSF-mediated actions on behalf of that authorized administrator. If RADIUS or TACACS is not configured or available, the TOE performs identification and authentication before allowing any other TSF-mediated actions on behalf of that authorized administrator

- FIA_UID.2: The TSF requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs through a secure connection (SSHv2 session with CLI, local console connection with CLI, SNMPv3, or XML API). The TOE provides the ability to securely manage: all TOE administrative users; all audit functionality of the TOE; all TOE cryptographic functionality; and the information flow control policies enforced by the TOE.

The TOE operates in two planes: the administration (admin) plane; and the Secure Domain Router (SDR) plane. SDRs are a means of dividing a single physical system into multiple logically separated routers. SDRs are isolated from each other in terms of their resources, performance, and availability. The admin plane consists of resources shared across all SDRs, while the SDR plane consists of those resources specific to the particular SDR.

TOE administrative users are classified into one of three categories:

- Root system user—functions with the highest privileges over all router components and can monitor all SDRs configured in the TOE. Multiple root system users can exist, and at least one root system user account must be created during router setup. A root system user can perform any configuration or monitoring task on the TOE
- Root SDR user—controls the configuration and monitoring of a specific SDR. The root SDR user can create users and configure their privileges within the SDR. Multiple root SDR users can work independently. A single SDR may have more than one root SDR user
- SDR user—has restricted access to an SDR as determined by a root system user or root SDR user. The SDR user performs day-to-day system and network management activities. The specific activities an SDR user is allowed to perform are determined by the specific privileges associated with the user groups to which the SDR user belongs (see below for further details).

A root system user can create other root system users. Additionally, root system users can create and configure SDRs, and then create root SDR users. Root SDR users can, in turn, create additional root SDR users and also create SDR users.

Note that for the purposes of this evaluation, the privileges and permissions described in the default groups actually compose the roles for the security functionality. The categories above do not impact the ability to perform the security functionality of these roles.

The TOE uses “task permissions” to provide a fine-grained security management model. The operational tasks that enable administrative users to control, configure and monitor the TOE are represented by Task IDs. A Task ID defines the permissions necessary to run a command. Users are associated with sets of Task IDs (called task groups) that define the scope of their authorized access to the TOE. When a Task ID is assigned to a task group, the permissions associated with the Task ID within the task group are specified. The TOE defines the following four task permissions:

- Read—specifies a designation that permits only a read operation
- Write—specifies a designation that permits a change operation and implicitly allows a read operation
- Execute—specifies a designation that permits an access operation (e.g., ping)
- Debug—specifies a designation that permits a debug operation.

As an example of how this mechanism operates within the TOE, consider the `acl` Task ID, which is required to be able to perform operations involving Access Control Lists. The administrator could create two task groups, one defining read-only permissions and the other defining read-write permissions. When assigning the `acl` Task ID to the read-only task group, the administrator would specify only the Read permission, whereas when assigning the `acl` Task ID to the read-write task group, the administrator would specify the Write permission (which also grants the read permission). A user associated with the read-only group would be able to run commands that only required

the Read permission on the `acl` Task ID (e.g., `show access-lists`), but could not run commands that required Write permission on the `acl` Task ID (e.g., `resequence access-list`).

Task groups are assigned to users through user groups. Each user is associated with one or more user groups, and every user group is associated with one or more task groups. Consequently, a user's association with a particular user group links that user to a particular set of Task IDs. A user that is associated with a Task ID can execute operations associated with that Task ID, within the scope of the assigned task permissions and their user category (i.e., root system, root SDR, or SDR user). That is, a root system user (either created at router setup or subsequently by another root system user) will be able to perform all commands for which their group assignments give them the appropriate Task IDs across the entire TOE, whereas a root SDR user (created by a root system or root SDR user) will be able to perform all commands for which their group assignments give them the appropriate Task IDs within the scope of their own SDR. Finally, an SDR user will be able to perform all commands for which their group assignments give them the appropriate Task IDs within the scope of their own SDR.

The TOE provides the following built-in or predefined user groups (along with associated task groups that have the same names and define the Task IDs and task permissions suitable to each user group):

- **root-system**—control and monitor the entire TOE
- **root-lr**—control and monitor a specific SDR
- **netadmin**—control and monitor system and network parameters tasks
- **sysadmin**—control and monitor all system parameters, but cannot configure network protocols
- **operator**—day to day monitoring activities and limited configuration rights
- **serviceadmin**—service administration tasks.

The TOE also defines a **cisco-support** user group, but this an add-on role that has no bearing on the Task IDs that support the TOE. It cannot be granted as the only role to a user, and it only impacts the cisco-support task ID which covers debugging capabilities. This role can be added onto either the root-lr or root-system group locally on the TOE, and to any user group when configured via TACACS or RADIUS. It is considered non-interfering with the security functionality that is part of this evaluation.

In addition to these predefined user and task groups, administrators can configure user groups and task groups to meet the particular needs of their installation. User groups and task groups can also inherit attributes from other user and task groups, respectively. For example, if user group A inherits from user group B, the new set of task attributes of user group A is the union of A and B (note that cyclic inclusions are detected and rejected). The inheritance relationship among user groups is dynamic—if group A inherits from group B, a change in group B propagates to group A, even if group A is not re-inherited explicitly. Also, user groups cannot inherit from any of the predefined user groups, but task groups can inherit from the predefined task groups.

A root-system administrator, or an administrator with `aaa` Task ID, can revoke a user's security role by removing their user group association. This revocation is enforced the next time the user attempts to login to the TOE.

The TOE defines a large number of Task IDs that together control all aspects of the security management function. For the purposes of evaluation, however, the following are the security-relevant Task IDs, the ones that provide access to security management capabilities as specified by the SFRs in this ST:

- logging—controls access to all commands associated with viewing audit records and managing the behavior of the security audit function
- acl—controls access to all commands associated with the management of access lists, which define the rule sets for the information flow control policies enforced by the TOE, including ICMP
- aaa—controls access to all commands associated with management of the I&A security function, including management of user accounts and association of users with security management roles via assigned user groups
- host-services—controls access to all commands associated with management of the TOE's clock

- tty-access—controls access to commands associated with the configuration and management of remote access
- crypto—controls access to commands associated with cryptographic operations.

6.1.5.1 Security function summary

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

- FMT_MOF.1(1): The TOE restricts the ability to manage all aspects of the Security Audit security function to root-system, sysadmin, netadmin, and administrators assigned the `logging` Task ID
- FMT_MOF.1(2): The TOE restricts the ability to enable and disable icmp to root-system, root-lr, netadmin, sysadmin, and administrators assigned the `acl` Task ID
- FMT_MSA.1: The TOE enforces its information flow policies to restrict the ability to manage the related security attributes to root-system, root-lr, netadmin, sysadmin, and administrators assigned the `acl` Task ID
- FMT_MSA.3: The TOE enforces its information flow policies to provide restrictive default values for security attributes that enforce the policies, and allows root-system, root-lr, netadmin, sysadmin, and administrators assigned the `acl` Task ID to specify alternative initial values for security attributes
- FMT_MTD.1(1): The TOE restricts the ability to manage time and date used to form the time stamps query to root-system, root-lr, netadmin, sysadmin, and administrators assigned the `host-services` Task ID
- FMT_MTD.1(2): The TOE restricts the ability to manage Access Control Lists to root-system, root-lr, netadmin, sysadmin, and administrators assigned the `acl` Task ID
- FMT_REV.1: The TOE restricts the ability to revoke security attributes associated with the information flow policy rule sets to root-system, root-lr, netadmin, sysadmin and administrators assigned the `acl` Task ID. Additionally, the TOE restricts the ability to revoke a user's security role (through their user group association) to root-system and administrators assigned the `aaa` Task ID
- FMT_SMF.1: The TOE provides administrators with the capabilities to manage the security of the TOE, as listed above, via the CLI
- FMT_SMR.1: The TOE provides predefined user groups and task groups that together implement security management roles, as well as a fine-grained security management model based on Task IDs associated with every CLI command.

6.1.6 Trusted Path/Channel

The TOE establishes a trusted path between itself and the remote management station used by the administrators to manage the TOE. This Trusted path is secured using an SSHv2 secure connection. All remote administration occurs through the secure trusted path (CLI over SSHv2, SNMPv3 with authentication, or XML API over SSLv3 or SSHv2). The SSHv2 session is encrypted and secure integrity-verified using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE. Alternatively, the TOE supports local administration through a directly connected management station.

The TOE establishes a trusted channel between itself and another trusted IT product; the authentication servers.

6.1.6.1 Security function summary

The Trusted Path/Channel function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: The TSF provides a secure, logically distinct communication channel between itself and another trusted IT product that provides assured identification of its end points and protection of the channel data from modification or disclosure. The TSF itself can initiate communication via the trusted channel. The TSF initiates communication via the trusted channel for all authentication decisions delegated to a remote authentication server

- FTP_TRP.1(1): The TSF provides an encrypted communication path between itself and remote authenticated administrative users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure. The TSF permits administrative users to initiate communication via the trusted path. The TSF requires the use of the trusted path for initial user authentication and all remote administration actions.
- FTP_TRP.1(2): The TSF uses cryptographic signatures to provide a communication path between itself and administrative users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from undetected of the modification of data. The TSF permits administrative users to initiate communication via the trusted path. The TSF requires the use of the trusted path for initial user authentication and all remote administration actions.

6.1.7 TOE Access

When an administrative session is initially established, the TOE displays a configurable warning banner. This is used to provide any information deemed necessary by the administrative personnel.

The TOE terminates a remote administrative session after a configurable amount of idle time. The amount of idle time required to terminate a remote administrative session is configurable by administrative users in the root-system, netadmin, or sysadmin roles, or assigned the `tty-access` Task ID. The administrator can set the time to any value between 0 and 35791 minutes (where 0 disables TSF-initiated session termination). The default value is 10 minutes.

The TOE provides the ability to deny administrative access to the TOE management CLI based on the location (IP address) of the requesting administrator, and the connecting network interface.

6.1.7.1 Security function summary

The TOE Access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3.1: The TSF terminates an interactive session after an administrator configurable time interval of session inactivity.
- FTA_TAB.1: Before establishing a user session, the TSF displays an advisory warning message regarding unauthorized use of the TOE.
- FTA_TSE.1: The TOE provides the ability to deny administrative access to the TOE management CLI based on the location (IP address) of the requesting administrator, and the connecting network interface.

6.1.8 Protection of the TSF

The TOE is capable of preserving a secure state when software or hardware failures occur. Whenever any failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE. This functionally prevents any failure from causing an unauthorized information flow. There are no failures that circumvent this protection. Whenever the TOE experiences a fault from which it cannot automatically recover, the TOE enters a safe state that allows the administrators to return the TOE to an operational state. The TOE provides the ability to automatically recover from a single fault in either the active RP/RSP or standby RP/RSP for TOE configurations that include dual RPs or RSPs. This includes the ability to handle both hardware and software failures. All other faults result in the TOE ceasing interface transmissions until the fault is addressed by user interaction (e.g., replacement of faulty hardware components, investigation and resolution by Cisco technical support). Once the problem that caused the TOE to cease operation and enter maintenance mode has been resolved, the administrator can reboot the TOE. All configured interfaces are automatically enabled as part of the boot process.

The TOE establishes a trusted channel between itself and another trusted IT product; the authentication servers. This ensures TSF data transmitted between the TOE and the authentication server is protected from disclosure and undetected modification. This connection is protected using SSL. If modifications are detected, the information is disregarded.

The TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records.

For TOE configurations that include dual RSPs or RPs one of the processors acts as the active hardware while the other acts as a hot standby. If there is a hardware failure within the active processor, the hot standby processor within the TOE automatically becomes active. If there is a software failure within the active software instance, the TOE automatically switches to the hot standby software instance resident within the TOE on the hot standby.

6.1.8.1 Security function summary

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

- FPT_FLS.1: The TSF preserves a secure state in the event of any failures
- FPT_ITC.1: The TSF protects all TSF data transmitted from itself to another trusted IT product from unauthorized disclosure during transmission
- FPT_ITI.1: The TSF provides the capability to detect modification and verify integrity of all TSF data during transmission between itself and another trusted IT product. If modifications are detected, the information is disregarded
- FPT_RCV.2: When automated recovery from failure or service discontinuity is not possible, the TSF enters a maintenance mode where the ability to return to a secure state is provided. The TSF ensures the return of the TOE to a secure state using automated procedures for dual RPs and dual RSPs
- FPT_STM.1: The TSF provides reliable time stamps for its own use
- FPT_HA_(EXT).1.1: The TSF provides hardware failover for any single hardware or software fault within the TSF for any TOE configuration which includes dual RPs/RSPs.

7. Protection Profile Claims

This Security Target makes no Protection Profile claim.

8. Rationale

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

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

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

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

Table 7: Environment to Objective Correspondence

	T. ADMIN_ERROR	T.AUDIT_COMPROMISE	T.MASQUERADE	T.SPOOFING	T.TSF_COMPROMISE	T.UNACCOUNTABILITY	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_USAGE	T.UNAVAILABILITY	T.UNIDENTIFIED_ACTIONS	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.NO_TOE_BYPASS	A.EXTERNAL_AUTH
O.AUDIT_GENERATION						X					X				
O.AUDIT_PROTECTION		X													
O.AUDIT_REVIEW											X				
O.AUTHENTICATION						X									
O.CRYPTO_FUNCTIONS					X										
O.DISPLAY_BANNER									X						
O.IDENTIFICATION						X									
O.MANAGE	X														
O.MEDIATE								X							
O.PROTECTED_COMMS					X										
O.SERVICE_CONTINUITY										X					
O.TOE_ACCESS			X				X								
O.TRUSTED_PATH			X	X											

	T. ADMIN_ERROR	T.AUDIT_COMPROMISE	T.MASQUERADE	T.SPOOFING	T.TSF_COMPROMISE	T.UNACCOUNTABILITY	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_USAGE	T.UNAVAILABILITY	T.UNIDENTIFIED_ACTIONS	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.NO_TOE_BYPASS	A.EXTERNAL_AUTH
OE.NO_GENERAL_PURPOSE												X			
OE.PHYSICAL													X		
OE.NO_TOE_BYPASS														X	
OE.EXTERNAL_AUTH															X

8.1.1.1 T.ADMIN_ERROR

An administrator may incorrectly configure or manage the TOE, resulting in ineffective security mechanisms.

This Threat is addressed by the following TOE security objectives:

- O.MANAGE—addresses this threat by providing administrators the tools necessary to configure and manage the TOE security functions, including the capability to view configuration settings. For example, if an administrator makes a mistake when configuring an information flow rule set, providing them the capability to view the rules affords them the ability to review the rules and discover any mistakes that might have been made

8.1.1.2 T.AUDIT_COMPROMISE

A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's actions.

This Threat is addressed by the following TOE security objectives:

- O.AUDIT_PROTECTION—addresses this threat by protecting audit information stored in the audit trail from unauthorized access. Only those authorized to do so by the TSF are able to read the audit trail and no modifications can be made to audit records stored in the audit trail.

8.1.1.3 T.MASQUERADE

A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.

This Threat is addressed by the following TOE security objective:

- O.TRUSTED_PATH—ensures the communication path end points between the TOE and authorized users are defined. This mechanism allows the TOE to be assured that it is communicating with an authorized IT entity
- O.TOE_ACCESS—addresses this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE

8.1.1.4 T.SPOOFING

An entity may misrepresent itself as the TOE to obtain authentication data.

This Threat is addressed by the following TOE security objective:

- O.TRUSTED_PATH—it is possible for an entity other than the TOE to provide an environment that may lead a user to mistakenly believe they are interacting with the TOE, thereby fooling the user into divulging identification and authentication information. This security objective mitigates this threat by providing users the capability to ensure they are communicating with the TOE when providing identification and authentication data to the TOE.

8.1.1.5 T.TSF_COMPROMISE

An attacker able to observe network communications between the TOE and remote administrators or remote IT entities may compromise TSF data.

This Threat is addressed by the following TOE security objectives:

- O.PROTECTED_COMMS—ensures the TOE is able to protect the TSF data it communicates with remote administrators and remote IT entities from unauthorized disclosure and undetected modification
- O.CRYPTO_FUNCTIONS—supports O.PROTECTED_COMMS by ensuring the TOE has the cryptographic capabilities necessary to encrypt and sign data, thus providing the mechanisms that enable the TOE to protect its communicated data from disclosure or undetected modification.

8.1.1.6 T.UNACCOUNTABILITY

The authorized users of the TOE may not be held accountable for their actions within the TOE, resulting in unauthorized and undetected activities that compromise the TOE or the data it protects.

This Threat is addressed by the following TOE security objectives:

- O.AUDIT_GENERATION—addresses this threat by providing the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE
- O.IDENTIFICATION—supports addressing this threat by requiring all users of the TOE identify themselves before being granted access to other TSF-mediated capabilities. The user identity is used to associate users with the auditable actions in the audit trail that they caused
- O.AUTHENTICATION—supports addressing this threat by requiring administrative users and authorized remote IT entities to authenticate their claimed identities to the TOE, thus providing assurance the audit records associated with users in the audit trail are associated with authenticated users of the TOE

8.1.1.7 T.UNATTENDED_SESSION

A user may gain unauthorized access to an unattended session.

This Threat is addressed by the following TOE security objective:

- O.TOE_ACCESS—addresses this threat by providing mechanisms that place controls on users' sessions. Administrators' remote sessions are dropped after an administrator defined time period of inactivity. This reduces the risk of someone accessing the TOE where the session was established, thus gaining unauthorized access to the session.

8.1.1.8 T.UNAUTHORIZED_ACCESS

A user sending data to or through the TOE may gain access to services for which they are not authorized according to the TOE security policy.

This Threat is addressed by the following TOE security objective:

- O.MEDIATE—addresses this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. Information flow rules ensure that the network identifier in a

packet is in the set of network identifiers associated with a TOE's network interface and provide increased granularity of access control by enabling the administrator to control the source and destination address, destination port, and protocol. Additionally, the TOE maintains "state" information of all approved connections, ensuring that each packet arriving at a TOE interface is checked against a current and valid list of connection parameters prior to allowing the packet through the TOE.

8.1.1.9 T.UNAUTHORIZED_USAGE

Through ignorance, a user may make inappropriate or unauthorized use of the TOE or use it in a fashion that is contrary to the site security policy.

This Threat is addressed by the following TOE security objective:

- O.DISPLAY_BANNER—addresses this threat by providing the TOE a mechanism to display to the user an advisory message warning about acceptable use of the TOE prior to the user establishing an administrative session with the TOE. This provides the administrator a capability to configure an appropriate warning message about what constitutes acceptable use of the TOE, which is visible to any user who may attempt to logon to the TOE and is displayed before any login attempt can be made.

8.1.1.10 T.UNAVAILABILITY

Hardware or software failures could cause the TOE to cease operating, resulting in its services being unavailable to authorized users.

This Threat is addressed by the following TOE security objective:

- O.SERVICE_CONTINUITY—addresses this threat by ensuring the TOE has mechanisms to support continuity of TOE services in the event of a failure.

8.1.1.11 T.UNIDENTIFIED_ACTIONS

The administrator may fail to notice potential security violations of the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

This Threat is addressed by the following TOE security objectives:

- O.AUDIT_GENERATION—addresses this threat by providing the audit mechanism to record security relevant events occurring on the TOE.
- O.AUDIT_REVIEW—supports O.AUDIT_GENERATION in addressing this threat by providing the administrators with a search capability that provides an efficient mechanism for the administrator to view audit information in order to identify possible security violations.

8.1.1.12 A.NO_GENERAL_PURPOSE

The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.

This Assumption is covered by the following security objective for the operational environment:

- OE.NO_GENERAL_PURPOSE—this objective ensures those responsible for the TOE in its operational environment will ensure there are no general purpose computing or storage repository capabilities available on the TOE.

8.1.1.13 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

This Assumption is covered by the following security objective for the operational environment:

- OE.PHYSICAL—this objective ensures those responsible for the TOE in its operational environment will ensure the operational environment provides physical security for the TOE commensurate with the value of the TOE and the data it contains.

8.1.1.14 A.NO_TOE_BYPASS

Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

This Assumption is covered by the following security objective for the operational environment:

- OE.NO_TOE_BYPASS—this objective ensures those responsible for the TOE in its operational environment will ensure information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

8.1.1.15 A.EXTERNAL_AUTH

The TOE can utilize external RADIUS or TACACS+ authentication servers..

This Assumption is covered by the following security objective for the operational environment:

- OE.EXTERNAL_AUTH —this objective ensures those responsible for the TOE in its operational environment will provide the external authentication server.

8.2 Security Functional Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the requirements in the Security Target.

8.2.1 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 that it is intended to satisfy.

Table 8: Objectives to Requirement Correspondence

	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUTHENTICATION	O.CRYPTO_FUNCTIONS	O.DISPLAY_BANNER	O.IDENTIFICATION	O.MANAGE	O.MEDIATE	O.PROTECTED_COMMS	O.SERVICE_CONTINUITY	O.TOE_ACCESS	O.TRUSTED_PATH
FAU_GEN.1	X												
FAU_GEN.2	X												
FAU_SAR.1			X										
FAU_SAR.2		X											
FAU_SAR.3			X										
FAU_STG.1		X											
FCS_CKM.1(1)					X								
FCS_CKM.1(2)					X								
FCS_CKM.1(3)					X								
FCS_CKM.4					X								

	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUTHENTICATION	O.CRYPTO_FUNCTIONS	O.DISPLAY_BANNER	O.IDENTIFICATION	O.MANAGE	O.MEDIATE	O.PROTECTED_COMMS	O.SERVICE_CONTINUITY	O.TOE_ACCESS	O.TRUSTED_PATH
FCS_COP.1(1)					X								
FCS_COP.1(2)					X								
FCS_COP.1(3)					X								
FCS_COP.1(4)					X								
FCS_COP.1(5)					X								
FDP_IFC.1(1)									X				
FDP_IFF.1(1)									X				
FDP_IFF.1(2)									X				
FIA_ATD.1				X			X					X	
FIA_UAU.1				X									
FIA_UAU.5				X									
FIA_UID.2							X						
FMT_MOF.1(1)								X					
FMT_MOF.1(2)								X					
FMT_MSA.1								X					
FMT_MSA.3								X					
FMT_MTD.1(1)								X					
FMT_MTD.1(2)								X					
FMT_REV.1								X					
FMT_SMF.1								X					
FMT_SMR.1								X					
FPT_HA_(EXT).1											X		
FPT_FLS.1											X		
FPT_ITC.1										X			
FPT_ITI.1										X			
FPT_RCV.2											X		
FPT_STM.1	X												
FTA_SSL.3												X	

	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUTHENTICATION	O.CRYPTO_FUNCTIONS	O.DISPLAY_BANNER	O.IDENTIFICATION	O.MANAGE	O.MEDIATE	O.PROTECTED_COMMS	O.SERVICE_CONTINUITY	O.TOE_ACCESS	O.TRUSTED_PATH
FTA_TAB.1						X							
FTA_TSE.1												X	
FTP_ITC.1													X
FTP_TRP.1(1)													X
FTP_TRP.1(2)													X

8.2.1.1 O.AUDIT_GENERATION

The TOE shall provide the capability to detect, and create records of, security-relevant events associated with the operation of the TOE.

This TOE Security Objective is met by the following SFRs:

- FAU_GEN.1—defines the set of events that the TOE must be capable of recording. This requirement ensures that the TOE has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event
- FAU_GEN.2—ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated
- FPT_STM.1—provides support in satisfying this objective by requiring the TOE provide reliable time stamps, which are used by the TOE when generating audit records.

8.2.1.2 O.AUDIT_PROTECTION

The TOE shall protect audit information stored in the audit trail from unauthorized access.

This TOE Security Objective is met by the following SFRs:

- FAU_SAR.2—restricts the ability to read the audit trail to administrators, thus preventing the disclosure of the audit data to any other user
- FAU_STG.1—protects the audit records from unauthorized modification or deletion, thus ensuring the integrity of the audit trail is maintained.

8.2.1.3 O.AUDIT_REVIEW

The TOE shall provide administrators the capability to selectively view audit information stored in the audit trail.

This TOE Security Objective is met by the following SFRs:

- FAU_SAR.1—provides the administrators with the capability to read all audit data contained in the audit trail. This requirement also mandates the audit information be presented in a manner that is suitable for the administrators to interpret the audit trail
- FAU_SAR.3—supports FAU_SAR.1 by providing the administrators the flexibility to specify criteria that can be used to search the audit records residing in the audit trail. It requires the administrators be able to establish the audit review criteria based on user identity and source subject identity, so that the actions of a user can be readily identified and analyzed.

8.2.1.4 O.AUTHENTICATION

The TOE shall be able to authenticate the claimed identities of administrative users and authorized IT entities.

This TOE Security Objective is met by the following SFRs:

- FIA_UAU.1—requires users to be successfully authenticated before the TSF will allow any other TSF-mediated actions to be performed on their behalf, with the exception of the unauthenticated information flow policy and unauthenticated TOE services specified by FDP_IFC.1a and FDP_IFC.1b
- FIA_UAU.5—requires that the TOE provide a local authentication mechanism and also be able to support an external authentication mechanism. These mechanisms are used by the TOE to authenticate the claimed identities of administrative users and authorized IT entities
- FIA_ATD.1(1)—supports the other SFRs by defining the attributes of users, including an identifier that is used to by the TOE to determine a user's identity and authentication data that is to be presented by the user to authenticate their claimed identity to the TOE.

8.2.1.5 O.CRYPTO_FUNCTIONS

The TOE shall provide cryptographic functions to support its security functions.

This TOE Security Objective is met by the following SFRs:

- FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3)—requires the TOE to provide cryptographic operations that support symmetric data encryption and decryption, digital signature services, and cryptographic key agreement services
- FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3)—requires the TOE be able to generate the symmetric and asymmetric keys necessary for it to support its cryptographic functions
- FCS_COP.1(4)—requires the TOE to implement SSH-2 using the cryptographic operations specified by FCS_COP.1(1), FCS_COP.1(2) and FCS_COP.1(3). Furthermore, the TOE will utilize the cryptographic keys it generates in accordance with FCS_CKM.1(1), FCS_CKM.1(2) and FCS_CKM.1(3)
- FCS_COP.1(5)—requires the TOE to implement SSLv3 using the cryptographic operations specified by FCS_COP.1(1), FCS_COP.1(2) and FCS_COP.1(3). Furthermore, the TOE will utilize the cryptographic keys it generates in accordance with FCS_CKM.1(1), FCS_CKM.1(2) and FCS_CKM.1(3)
- FCS_CKM.4—requires the TOE be able to destroy cryptographic keys after they no longer required.

8.2.1.6 O.DISPLAY_BANNER

The TOE shall display an advisory warning regarding use of the TOE.

This TOE Security Objective is met by the following SFRs:

- FTA_TAB.1—meets this objective by requiring the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under control of the administrators, in which they specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire.

8.2.1.7 O.IDENTIFICATION

The TOE shall be able to identify all users of the TOE.

This TOE Security Objective is met by the following SFRs:

- FIA_UID.2—meets this objective by ensuring that every user is identified before the TOE performs any mediated functions. In some cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication, in which case the identity is presumed to be authentic). In other cases (e.g., administrators and authorized IT entities), the identity of the user is authenticated
- FIA_ATD.1(1)—supports FIA_UID.2 by defining the attributes of administrative users including an identifier that is used to by the TOE to determine a user's identity and authentication data that is to be presented by the user to authenticate their claimed identity to the TOE.

8.2.1.8 O.MANAGE

The TOE shall provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

This TOE Security Objective is met by the following SFRs:

- FMT_SMF.1—requires the TOE to provide the functions and facilities necessary for the administrators to manage the security of the TOE
- FMT_SMR.1—supports FMT_SMF.1 by defining the security management roles to be provided by the TOE. Other FMT requirements specify how security management capabilities are to be restricted to the defined roles
- FMT_MOF.1(1)—supports FMT_SMF.1 by specifying how management of the security audit function is to be restricted to defined roles
- FMT_MOF.1(2)—supports FMT_SMF.1 by specifying how management of the unauthenticated TOE services is to be restricted to defined roles
- FMT_MSA.1—supports FMT_SMF.1 by specifying how management of the security attributes associated with enforcement of the unauthenticated information flow control and unauthenticated TOE services SFPs are to be restricted to defined roles
- FMT_MSA.3—supports FMT_SMF.1 by specifying how security attributes associated with enforcement of the unauthenticated information flow control and unauthenticated TOE services SFPs are to be initialized, and what roles are able to specify alternative initial values for those attributes
- FMT_MTD.1(1)—supports FMT_SMF.1 by specifying how management of system time stamps is to be restricted to defined roles
- FMT_MTD.1(2)—supports FMT_SMF.1 by specifying how management of the information flow policy rules is to be restricted to defined roles
- FMT_REV.1—supports FMT_SMF.1 by specifying how security attributes are to be revoked and how such revocation is to be restricted to defined roles.

8.2.1.9 O.MEDIATE

The TOE shall mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.

This TOE Security Objective is met by the following SFRs:

- FDP_IFC.1(1)—defines the subjects, information and operations that are performed with respect to the unauthenticated information flow policy that controls the flow of information between sets of TOE network interfaces

- FDP_IFF.1(1)—specifies the policy of unauthenticated traffic flowing through the TOE. This requirement ensures that the network traffic is mediated (i.e., the rule set is used) even though the subjects have not been authenticated. This requirement also mandates the TOE perform stateful inspection of the packets to determine if they should be allowed to flow through the TOE. The stateful inspection attributes are not intended to specifiable by the administrator—rather these attributes are to be controlled and mediated internally by the TOE
- FDP_IFC.1(2)—defines the subjects, information and operations that are performed with respect to the unauthenticated TOE services policy that controls the flow of information between a network interface and the TOE itself
- FDP_IFF.1(2)—specifies the rules that apply to the unauthenticated use of any services provided by the TOE. ICMP is the only unauthenticated service that is provided by the TOE, and the security attributes associated with this protocol allow the administrator to specify what degree the ICMP traffic is mediated (i.e., the ICMP message type and code).

8.2.1.10 O.PROTECTED_COMMS

The TOE shall be able to protect its communications with authorized remote IT entities from unauthorized disclosure and undetected modification.

This TOE Security Objective is met by the following SFRs:

- FPT_ITC.1—specifies the TOE protects all TSF data it transmits to another trusted IT product from unauthorized disclosure during transmission. The TOE utilizes the cryptographic capabilities specified to meet O.CRYPTO_FUNCTIONS in order to encrypt the data it transmits to authorized remote IT entities
- FPT_ITI.1—specifies the TOE is able to detect any modifications to TSF data transmitted between it and another trusted IT product, and will disregard any such information when modification is detected. The TOE utilizes the cryptographic capabilities specified to meet O.CRYPTO_FUNCTIONS in order to digitally sign data it transmits to authorized remote IT entities and to verify digital signatures applied to the data it receives from authorized remote IT entities.

8.2.1.11 O.SERVICE_CONTINUITY

The TOE shall provide capabilities to support continuity of TOE services in the event of a failure.

This TOE Security Objective is met by the following SFRs:

- FPT_HA_(EXT).1—specifies the TOE provides failover for any single hardware or software failure in TOE configurations that include dual redundant Route Switch Processors. This ensures such TOEs are able to maintain routing capability in the event of a failure
- FPT_RCV.2—provides support in meeting this objective by requiring the TOE to automatically recover from any single software or hardware failure of an RSP, and by additionally requiring that the TOE provide a maintenance mode from which return to a secure state is possible, in the event automated recovery is not possible
- FPT_FLS.1—provides support in meeting this objective by requiring the TOE to preserve a secure state in the event of any failures.

8.2.1.12 O.TOE_ACCESS

The TOE shall provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.

This TOE Security Objective is met by the following SFRs:

- FIA_ATD.1—supports FIA_AFL.1 by associating with each user a username, password, and role
- FTA_SSL.3—contributes to satisfying this objective by ensuring that users' sessions are afforded some level of protection. After an administrator defined time interval of inactivity, interactive sessions will be terminated

- FTA_TSE.1—contributes to satisfying this objective by limiting a user's ability to logically access the TOE. This requirement provides the administrator the ability to control when (e.g., time and day(s) of the week) and where (e.g., from a specific network address) remote administrators can access the TOE.

8.2.1.13 O.TRUSTED_PATH

The TOE shall provide a means to ensure administrative users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.

This TOE Security Objective is met by the following SFRs:

- FTP_TRP.1(1), FTP_TRP.1(2)—require the TOE to provide a mechanism that creates a distinct communication path that protects the data that traverses this path from disclosure or modification. This requirement ensures that the TOE can identify the end points and ensures that a user cannot insert themselves between the user and the TOE, by requiring that the means used for invoking the communication path cannot be intercepted and allow a "man-in-the-middle-attack". Since the user invokes the trusted path (FTP_TRP.1.2) mechanism, they can be assured they are communicating with the TOE. FTP_TRP.1.3 mandates that the trusted path be the only means available for providing identification and authentication information, therefore ensuring a user's authentication data will not be compromised when performing authentication functions. Furthermore, the remote administrator's communication path is encrypted during the entire session
- FTP_ITC.1—require a mechanism that creates a distinct communication path to protect communications with IT entities from disclosure or modification. FTP_ITC.1.3 requires the TOE to initiate the trusted channel, which ensures that the TOE has established a communication path with an authorized IT entity and not some other entity pretending to be an authorized IT entity.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 augmented with ALC_FLR.2 assurance package. The TOE has been developed based on good commercial development practices for a generalized environment with a low level of risk to the assets it protects. The security environment assumes physical protection commensurate with the value of the TOE and the assets it protects. As such, it is believed that EAL3 augmented with ALC_FLR.2 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

Table 9: Requirement Dependencies

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1(1)	FCS_CKM.4, FCS_CKM.2 or FCS_COP.1	FCS_CKM.4, FCS_COP.1
FCS_CKM.1(2)	FCS_CKM.4, FCS_CKM.2 or FCS_COP.1	FCS_CKM.4, FCS_COP.1
FCS_CKM.1(3)	FCS_CKM.4, FCS_CKM.2 or FCS_COP.1	FCS_CKM.4, FCS_COP.1
FCS_CKM.4	FCS_CKM..1 or FDP_ITC.1, or FDP_ITC.2	FCS_CKM..1

ST Requirement	CC Dependencies	ST Dependencies
FCS_COP.1(1)	FCS_CKM.4, FCS_CKM..1 or FDP_ITC.1, or FDP_ITC.2	FCS_CKM.4, FCS_CKM..1
FCS_COP.1(2)	FCS_CKM.4, FCS_CKM..1 or FDP_ITC.1, or FDP_ITC.2	FCS_CKM.4, FCS_CKM..1
FCS_COP.1(3)	FCS_CKM.4, FCS_CKM..1 or FDP_ITC.1, or FDP_ITC.2	FCS_CKM.4, FCS_CKM..1
FCS_COP.1(4)	FCS_CKM.4, FCS_CKM..1 or FDP_ITC.1, or FDP_ITC.2	FCS_CKM.4, FCS_CKM..1
FCS_COP.1(5)	FCS_CKM.4, FCS_CKM..1 or FDP_ITC.1, or FDP_ITC.2	FCS_CKM.4, FCS_CKM..1
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1(1), FMT_MSA.3
FDP_IFF.1(2)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1(2), FMT_MSA.3
FIA_ATD.1	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	None
FIA_UID.2	none	None
FMT_MOF.1(1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MOF.1(2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	FMT_SMF.1, FMT_SMR.1, and FDP_ACC.1 or FDP_IFC.1	FMT_SMF.1, FMT_SMR.1, FDP_ACC.1, FDP_IFC.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1(2)	FMT_SMF.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_REV.1	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	none	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_FLS.1	None	None
FPT_ITC.1	None	None
FPT_ITI.1	None	None
FPT_RCV.2	AGD_OPE.1	AGD_OPE.1
FPT_STM.1	None	None
FTA_SSL.3	None	None
FTA_TAB.1	None	None
FTA_TSE.1	None	None
FTP_ITC.1	None	None
FTP_TRP.1(1)	None	None
FTP_TRP.1(2)	None	None
Explicitly Stated Security Functional Requirements		
FPT_HA_(EXT).1	None	None

8.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, 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. The following table demonstrates the relationship between security requirements and security functions.

Table 10: Security Functions vs. Requirements Mapping

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE Access	Trusted Path/Channels
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_SAR.3	X							
FAU_STG.1	X							
FCS_CKM.1(1)		X						
FCS_CKM.1(2)		X						
FCS_CKM.1(3)		X						
FCS_CKM.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_COP.1(5)		X						
FDP_IFC.1(1)			X					
FDP_IFC.1(2)			X					
FDP_IFF.1(1)			X					
FDP_IFF.1(2)			X					
FIA_ATD.1				X				
FIA_UAU.1				X				
FIA_UAU.5				X				
FIA_UID.2				X				
FMT_MOF.1(1)					X			
FMT_MOF.1(2)					X			
FMT_MSA.1					X			
FMT_MSA.3					X			
FMT_MTD.1(1)					X			
FMT_MTD.1(2)					X			
FMT_REV.1					X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_FLS.1						X		
FPT_HA_(EXT).1						X		
FPT_ITC.1						X		
FPT_ITI.1						X		

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE Access	Trusted Path/Channels
FPT_RCV.2						X		
FPT_STM.1						X		
FTA_SSL.3							X	
FTA_TAB.1							X	
FTA_TSE.1							X	
FTP_ITC.1								X
FTP_TRP.1(1)								X
FTP_TRP.1(2)								X

8.6 PP Claims Rationale

See Section 7, Protection Profile Claims.