Security target for Ericsson SmartEdge Series Router SE100, SE600, SE1200, SE1200H running SEOS ver 11.1 Software

Headquarters:
Ericsson AB,
Torshamnsgatan 23,
SE 164 80,
Stockholm, Sweden

R&D India Center:
Ericsson India Global Services Pvt Ltd,
Ground Floor, West Wing, Salarpuria Supreme,
Outer Ring Road, Marathahalli Junction,
Bangalore – 560037

Ericsson India Office Address:
Ericsson India Pvt Ltd,
Ericsson Forum,
DLF Cyberciti,
Sector 25A, Gurgaon
Haryana – 1220

127/1056-FCP 121 5927 Uen Rev K

Revision	Author(s)	Date	Approver	Description
A	Ravi H	28-09-11	Eric Magnusson	First version
C	Ravi YV, Suresh T, Ravi H	31-10-11	Eric Magnusson	Document upates – based on the feedback given by T. Bandyopadhyay of STQC (Ref: WS-ST-01_Ericsson_Router)
D	Suresh T, Kousik N, Ravi H, Ravi YV	30-11-11	Eric Magnusson	Document updates, based on the review comments received from STQC through the document – OR_ASE_22112011
E	Kousik N, Ravi YV	20-12-11	Eric Magnusson	More information on TOE description, FCS class introduction, Revised Threat mapping, addition of Extended component
F	Ravi YV	21-12-11	Eric Magnusson	Corrected entries in User levels table
G	Kousik N	06-01-12	Eric Magnusson	Modified as per the feedback provided in the Face-to-Face meetings.
H	Kousik N	31-01-12	Eric Magnusson	Incorporated as per the observation report
J	Kousik N	16-07-12	Y V Ravikumar	Incorporated as per the observation report on build 711
K	Kousik N	25-07-12	Eric Magnusson	Minor corrections to match TOE build 713

Contents

Contents – Tables and Figures

1 ST Introduction

1.1 ST and TOE Reference Identification

TOE Reference: SEOS 11.1*, running on* Ericsson SmartEdge Series Routers, SE 100, SE 600, SE 1200, SE1200H

SEOS 11.1 Build number: SEOS-11.1.2.3.713-Release

SEOS 11.1 Build Date: Fri Jun 22 01:07:50 PDT 2012

ST Reference: Security target for Ericsson SmartEdge Series Router SE100, SE600, SE1200, SE1200H running SEOS ver 11.1 Software.

ST Version: Revision K

Assurance Level: Evaluation Assurance Level (EAL) 3

ST Author: Ericsson

Keywords: Router, IP, Service Manager

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

The TOE is Ericsson SEOS 11.1, running on Smart Edge series of routers, as listed in section 1.1 of this document.

The TOE routes IP traffic over any type of network, with increasing scalability of the traffic volume with each TOE model. All packets on the monitored network are scanned and then compared against a set of rules that define the routing of the IP traffic.

The hardware TOE runs on are Ericsson Smart Edge series router SE100, SE600, SE1200 and SE1200H which have same functionality as far as security features are concerned. These hardware models vary in the type of physical interfaces, traffic processing capacity, memory and power consumption requirement but other functionalities, the configurations are the same.

1.2.2 Major security features of the TOE

The TOE supports the following security features:

1.2.2.1 Information Flow Function

The TOE is designed primarily to route IP network traffic. Network traffic represents information flows between source and destination network entities based on the routing configuration subject to the flow control rules setup by the Operator, Restricted-admin and Administrators.

1.2.2.2 Identification and Authentication Function

The TOE requires users to provide unique identification and authentication data (username, password) before any administrative access to the system is granted.

The SEOS software supports four methods of user authentication:

1. local password authentication (authentication against locally stored user name & user password)

2. local authentication using public key authentication (via the SSH application),

3. Authentication & authorization based on Remote Authentication Dial - In User Service (RADIUS)

4. Authentication & authorization based on Terminal Access Controller Access Control System Plus (TACACS).

1.2.2.3 Security Management Function

The TOE restricts the ability to administer the router's configuration entries to Restricted-admin and Administrators. The CLI provides a text based interface from which the router configuration can be managed and maintained. The following tasks can be performed by the Administrators from the CLI:

- Administer user attributes – create, modify or delete user accounts
- View or Manage audit logs

- Configure date/time settings
- Create, delete or modify the rules that control the presumed address from which management sessions can be established.

1.2.2.4 Audit Function

The TOE supports audit data generation for various events like successful user logins, logout, failed login attempts, configuration changes etc.

User identity association: Each audit record is associated with the identity of the user causing the event to ensure tracing the audit records against the user.

Only Restricted-operator, Operator, Restricted-admin and Administrators have the ability to review audit data from the CLI. Audit trail storage is also secured from modification by any user below Administrators.

1.2.2.5 TOE Access function

The TOE can be configured by Restricted-admin or Administrator through use of packet filters such that users can only gain access from specific management networks/stations at specific IP addresses.

All access attempts to the TOE require to pass through an authentication mechanism.

1.2.2.6 Clock Function

The clock function of the TOE provides a source of date and time information for the appliance, used in audit timestamps.

1.2.2.7 TOE Self-Test

The TOE performs a series of self-tests on startup, which checks the integrity of the TOE.

1.2.2.8 Trusted Recovery

The TOE high availability and process restorability are used for trusted recovery across processes and version upgrades.

1.2.2.9 Domain Separation

The TOE offers clear separation of data and control/management plane at its architecture ensuring TOE protection.

1.2.3 Operation environment of the TOE

The TOE is SEOS 11.1 running in any of the Ericsson Smart Edge series routers SE 100, SE 600 or SE 1200, SE1200H.

The major differences across the hardware models are summarized as:

Table 1 Capability comparison of the SE models

Product	SE100	SE600	SE1200, SE1200H
Traffic capacity	12Gbps	240Gbps	480Gbps
Number of subscribers supported	8000	256000	256000
Size in rack units	2	7	16
Major interface modules supported	12 10/100 Base T Ethernet, 2 1000 Base T Ethernet, 2 ATM OC-3	60 10/100 Base T Ethernet, 20 1000 Base T Ethernet, 4 10000 Base T Ethernet, 1 ATM OC-192, 4 ATM OC-48, 8 ATM OC-3	60 10/100 Base T Ethernet, 20 1000 Base T Ethernet, 4 10000 Base T Ethernet, 1 ATM OC-192, 4 ATM OC-3
Number of slots and line cards	Modular Interface cards fixed	8, 6	14, 12
Max Power consumption	300 watts	2736 watts	3840 watts, 5856 watts
Backplane card	1	2 in active/standby	2 in active/standby

The operation environment is the conditions favorable for the TOE to be able to provide all of its security functionality, with few assumptions on physical, personnel & operational aspects of the conditions surrounding the TOE.

1.3 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009, CCMB - 2009 - 07 - 001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 3, July 2009, CCMB - 2009 - 07 - 002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 3, July 2009, CCMB - 2009 - 07 - 003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB - 2009 - 07 - 004.

1.4 TOE Description

The TOE platforms are designed to provide an efficient and effective IP router/switch solution that can be managed centrally.

1.4.1 TOE Type

The TOE is the Smart Edge Operating System – SEOS 11.1, running on the Ericsson SmartEdge series routers, as listed in section 1.1 It provides routing services in a communication network.

1.4.2 Required non - TOE hardware/software/firmware

The TOE requires physical network interfaces to be installed to communicate with external network entities. These interfaces include the line-cards, XFP’s, FPGA, MAC, PMA & optical connectivity devices & drivers. However, these interfaces would be outside the TOE boundary.

1.4.3 SmartEdge Series Routers

SEOS 11.1 running on an Ericsson Smart Edge series routing platform is a complete routing system that supports Ethernet interfaces for medium/large networks and network applications. Ericsson routers share common SEOS software, features, and technology for compatibility across platforms.

The SmartEdge router is a carrier-class product, known as a Multi-Service Edge Router (MSER), with an architecture that supports packetized traffic. This router is considered "smart" as it combines different kinds of network traffic such as mobile, video, and so on and manages them in one single router. The 3 main system components are the chassis, controller cards, and traffic cards also known as Ethernet line cards.

The Ethernet line card, along side the cross connect controller card, is a key component of a SmartEdge router. The main function of the line card is to route IP/Ethernet traffic to its destination port, which can be a different port on the same card or a different port on a different card in the same chassis. The routing task is done by the Packet Processing ASIC (PPA) hardware, and the software that controls the card runs on the cross connect controller card.

The cross connect controller card runs the software that controls (TOE) the system and is responsible for the packet routing protocols, the SmartEdge OS command-line interface (CLI), and communications with a network management system running the NetOp™ Element Management System (EMS) software.

The architecture is a carrier-class or ISP-class product (depending on customer needs), targeted towards edge network markets. Its architecture simultaneously supports traditional time division multiplexed (TDM) traffic and packet-based IP traffic. Applications supported include point-to-point terminal, linear add-drop multiplexer (ADM), unidirectional path-switched ring (UPSR), 2-fiber / 4-fiber bi-directional line switched ring (BLSR), optical hub and stand-alone router. The architecture of the SE routers is fully redundant for all traffic-affecting components. SONET optical interfaces are protected on a 1+1 basis by independent working and protection circuit packs. Cross-connection and shelf processing functions are also protected by redundant circuit packs.

The router architecture of each platform cleanly separates routing and control functions from packet forwarding operations, thereby eliminating bottlenecks and permitting the router to maintain a high level of performance.

1.4.4 External IT Environment Components

The TOE can optionally use the service of external servers, for example, RADIUS and TACACS for authentication, NTP for time synchronization, Syslog for event logging. However the TOE is able to function even in the absence of these components.

1.5 TOE Boundaries

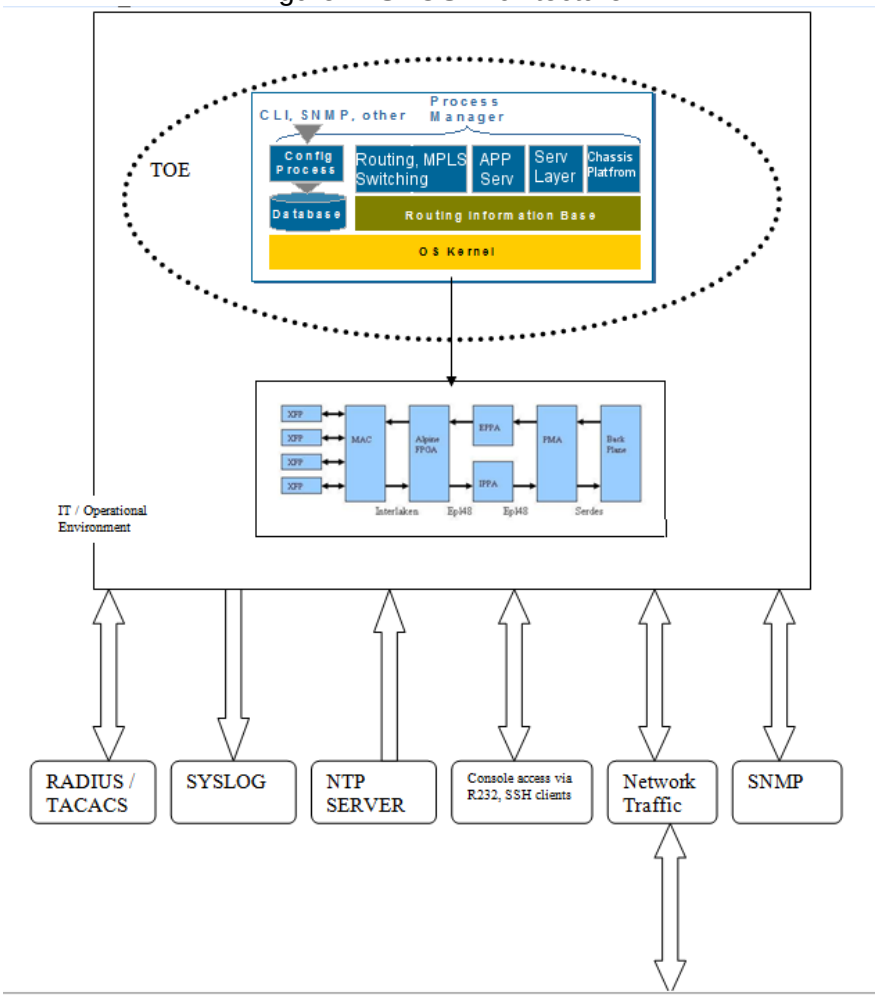
The physical and logical boundaries of the TOE are described as follows.

1.5.1 Physical Boundary

The TOE is a SEOS 11.1 which is a software operating within the physical boundary of the appliance.

The Ethernet Line Cards and other appliance hardware components along with their firmwares are outside the TOE boundary though they constitute the environment in which the TOE runs.

Figure 1 SEOS Architecture



The interfaces to the TOE are twofold: the routing interfaces and the management interfaces. The management interfaces include the TOE console interface through which the appliance can be managed locally.

1.5.2 Logical Boundaries

The logical boundaries of the TOE are defined by the functions that can be carried out by the TOE external interfaces. These functions include network information flow control, identification and authentication for the administrative functions, access control for administrative functions, management of the security configurations, audit and protection of the TOE itself.

Information Flow Control

The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users.

Identification and Authentication

The TOE requires users to provide unique identification and authentication information before any administrative access to the system is granted. TOE provides five levels of authority to the users (in increasing level of privilege) – Non-privileged user, Restricted-Operator, Operator, Restricted-Admin, and Administrator providing administrative flexibility.

The appliances also require that applications exchanging information with them successfully authenticate prior to any exchange. This covers all services used to exchange information, typically SSH.

Authentication services can be handled either internally (user selected passwords) or through a RADIUS or TACACS authentication server in the IT environment (the external authentication server is considered outside the scope of the TOE). For SSH only Public Key Authentication such as RSA can be used for the validation of the user credentials, but the user identity and privileges are still handled internally.

Security Management

The appliance is managed, including user management and the configuration of the router functions, through a Command Line Interface (CLI) protected by SSH. The CLI interface is accessible through an SSH session, or via a local terminal console.

Audit

SEOS auditable events are stored in the syslog files, and although they can be sent to an external log server, the requirements for auditing are met by local storage. Audit events cover authentication activity and configuration changes. Audit logs include the date and time, event category, event type & username. An accurate time is gained by the appliance ntp daemon, acting as a client, from an NTP server in the IT environment. This external time source allows synchronization of the TOE audit logs with external audit log servers in the environment.

Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routes. Another protection mechanism is that all routing functions of the TOE are confined to the appliance itself.

The TOE is completely self - contained, and maintains its own execution domain as follows:

- Each sub - component of the appliance software operates in an isolated execution environment, protected from accidental or deliberate interference by others.

- The entire software environment is protected from accidental or deliberate corruption via use of digitally signed binaries.

1.5.3 Summary of items out of the TOE boundary

There are no security functionality claims relating to the following items:

- All hardware, including that associated with forwarding interfaces & Line Cards.
- External servers (audit, NTP, authentication, FTP servers)

2 CC Conformance

CC Identification:

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009, CCMB - 2009 - 07 - 001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 3, July 2009, CCMB - 2009 - 07 - 002.

CC Part 2 (Version 3.1, Revision 3, July 2009) extended due to the use of the components FPT_DSP_EXT and FPT_TST_EXT

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 3, July 2009, CCMB - 2009 - 07 - 003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB - 2009 - 07 - 004.

ISO/IEC 15408-1 ed3.0 (2009-12)

ISO/IEC 15408-2 ed3.0 (2008-08)

ISO/IEC 15408-3.0 (2008-08)

This ST does not claim conformance to any PPs.

Ericsson attempts to get the SEOS 11.1 certified at EAL 3. This ST has been prepared to address the EAL3 certification requirements.

3 Security Problem Definition

The security problem definition (SPD) specifies threats, organizational security policies and assumptions concerning the TOE. The statement of TOE security environment defines the following:

Threats to be countered by the TOE, its operational environment, or a combination of the two;

Assumptions made on the operational environment in order to be able to provide security functionality;

Organizational security policies with which the TOE, its operational environment, or a combination of the two are to enforce.

3.1 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

Threat agents are entities that can adversely act on assets – the threat agents in the threats below are unauthorized user, network attacker, and authorized user.

Assets are entities that someone places value upon – the assets are access to network services,

Adverse actions are actions performed by a threat agent on an asset – the adverse actions are: unauthorized changes to configuration; both network routing configuration and management configuration.

The TOE protects IP packets against incorrect routing caused by unauthorized changes to the network configuration.

Table 2 Threats Table

T.ROUTE	Network packets may be routed inappropriately due to accidental or deliberate mis-configuration.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.

T.INTERCEPT	Unauthorized change to the management traffic to/from the TOE may be made through interception of traffic on a network.
T.CONFLOSS	Failure of network components may result in loss of configuration data that cannot quickly be restored.
T.NOAUDIT	Unauthorized changes to the TOE configurations and other management information may not be detected.
T.PROTECT	An unauthorized process or application may gain access to the TOE security functions and data, harming the security functions of the TOE

3.2 Organizational Security Policies

There are no organizational security policies that the TOE must meet.

3.3 Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.3.1 Physical Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3.2 Personnel Assumptions

A.NOEVIL The authorized users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.3.3 IT Environment Assumptions

A.EAUTH External authentication services will be available through either a RADIUS server or a TACACS server, or both.

A.TIME External NTP services will be available.

4 Security Objectives

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

Table 3 Objectives Table

O.FLOW	The TOE must ensure that network packets flow from source to destination according to defined routing information.
O.ACCESS	The TOE must only allow authorized users and processes (applications) to access protected TOE functions and data.
O.ROLBAK	The TOE must enable rollback of router configurations to a previously stored known state.
O.AUDIT	Users must be accountable for their actions in administering the TOE.
O.PROTECT	The TOE must protect against unauthorized accesses and disruptions of TOE functions and data – by separating user and control data planes
O.ENCRYPT	Encryption of management data in a remote management session

4.2 Security Objectives for the Environment

The following security objectives for the environment of the TOE must be satisfied in order to fulfill its own security objectives.

OE.EAUTH: A RADIUS server, a TACACS server, or both must be available for external authentication services.

OE.TIME: NTP server(s) must be available to provide accurate/synchronized time services to the router.

OE.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.

OE.ADMIN: Authorized users must follow all administrator guidance.

5 Extended Component Definition

This section describes the extended components defined for the TOE.

5.1 FPT_DSP_EXT

5.1.1 Requirement for Extended Component

Separation of the data and control planes ensures that the forwarding function of the TOE is not influenced by a user packet therefore protecting the TOE

5.1.2 Definition of the Extended Component

This extended component was defined because the part 2 of [ISO 15408-2] does not contain any SFR which addresses data and control plane separation. We are extending the Class FPT – TOE Protection Class, as this TSF ensures protection of the TOE – as follows:

The TOE ensures clear separation between control plane and data / forwarding plane. Control plane (aka BSD), contains processes that implement the protocols needed for the basic functionality of system, i.e, routing protocols, BRAS protocols, AAA, configuration management, NMS and so on. These processes run on separate processor in the XCRP as regular unix processes over a unix operating system (NetBSD).

A separate forwarding plane, responsible for the forwarding of the packet traffic and executes on a pair of multi-core packet processor asics (PPA) on each linecard. The PPAs consist of a number of cores, called execution units (EUs), which are general purpose processors augmented with a variety of hardware assists depending on the generation of the ASIC. The PPA EUs are logically grouped in two parts, EU0 and EU. The EU0 part that runs general purpose code mostly written in C language that processes configuration from the control plane and the forwarding EU part that handles the actual packet forwarding and contains code that in certain cases is written in assembly for higher performance.

The forwarding plane participates in the state machines of the control plane and creates its own state by receiving configuration messages. A clear separation between control and forwarding plane results in headless operation, i.e., the forwarding plane operates while the control plane is down & limits its execution within the scope of its plane independently. Communication between control and data plane happens only through well defined state machines for exchange of messages across separate planes.

Family Behavior

This family defines the need for separation of the user data and the control data. That would ensure that critical routing information in the TOE is protected against intentional / accidental corruption

Component Leveling

This family consists of only one component FPT_DSP_EXT.1

FPT_DSP_EXT: Data and control plane separation	1

5.1.3 Management: FPT_DSP_EXT.1

None

5.1.4 Audit: FPT_DSP_EXT.1

None

5.1.5 Dependency

This extended component has no decency and is not hierarchical to any other component.

5.1.6 FPT_DSP_EXT.1.1

The TOE shall ensure separation of the user data from the control data

5.1.7 Testability and Traceability

This extended component can be tested, verified and could be traced through the test cases that ensure the data traffic does not effect the control plane.

5.2 FPT_TST_EXT

5.2.1 Requirement for the Extended Component

In order to detect integrity failures of underlying security functionalities used by the TSF, the TOE will perform self-tests.

Existing family of the FPT_TST class as defined in CC part 2 does not address the requirement fully, hence the new extended component has been defined.

5.2.2 Definition

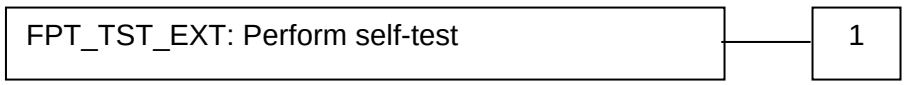
The TOE consists of a set of processes, corresponding to different functions such as – AAA, routing protocols etc. These processes are invoked by the process manager (PM). The PM checks the integrity of the process binaries, before starting the processes.

Family Behavior

This family addresses the need for self test by the TOE

Component leveling

This family consists of only one component.



5.2.3 Management: FPT_TST_EXT.1

None

5.2.4 Audit: FPT_TST_EXT.1

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

Basic: Results of the tests.

5.2.5 Dependency

This extended component has no dependency and is not hierarchical to any other component.

5.2.6 FPT_TST_EXT.1.1

The TOE shall perform the integrity checks on the daemon binaries.

5.2.7 Testability and Traceability

This extended component can be tested, verified and could be traced through the test cases that ensures the TOE runs a self-test to check integrity of binaries.

6 IT Security Requirements

6.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.
- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by [*italicized text within square brackets*].
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration sequence letter following the component identifier.

6.2 Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE, organised by CC class. Table 4 below identifies all SFRs implemented by the TOE. In the following table the components are listed, showing completed operations.

Table 4 Security Functional Components

Security Functional Class	Security Functional Components
Audit (FAU)	Security alarms (FAU_ARP.1)

	Audit review (FAU_SAR.1)
	Audit data generation (FAU_GEN.1)
	User identity association (FAU_GEN.2)
	Potential violation analysis (FAU_SAA.1)
	Protected audit trail storage (FAU_STG.1)
User data protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Authentication failure (FIA_AFL.1)
	Verification of secrets (FIA_SOS.1)
	User authentication before any action (FIA_UAU.2)
	Multiple authentication mechanisms (FIA_UAU.5)
	User identification before any action (FIA_UID.2)
Security management (FMT)	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (Router/Switch configuration) (FMT_MTD.1a)
	Management of TSF data (User attributes) (FMT_MTD.1b)
	Management of TSF data (Audit logs) (FMT_MTD.1c)
	Management of TSF data (Date/time) (FMT_MTD.1d)
	Management of TSF data (Sessions) (FMT_MTD.1e)
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Time stamps (FPT_STM.1)
	Self Test (FPT_TST_EXT.1)
	Trusted recovery (FPT_RCV.1)

	Separation of the data and management planes - (FPT_DSP_EXT.1)
	Recovery from failure (FPT_FLS.1)
TOE access (FTA)	TOE session establishment (FTA_TSE.1)
	Limit multiple concurrent sessions (FTA_MCS.1)
	Session Termination on Inactivity (FTA_SSL.3)
Cryptographic support (FCS)	Cryptographic key generation (FCS_CKM.1)
	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)

6.2.1 Audit (FAU)

6.2.1.1 Security alarms (FAU_ARP.1)

FAU_ARP.1.1

The TSF shall take [the following configurable actions: create a log entry and drop connection] upon detection of a potential security violation.

6.2.1.2 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

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

Start - up and shutdown of the audit functions;

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

[User login/logout;

Login failures;

Committing the TOE configuration;

Changing the TOE configuration];

Table 5 Audit Events

SFR Family	Description	Audit Event
FAU_ARP.1	Security audit automatic response	Actions taken due to potential security violations
FAU_GEN.1	Security audit data generation	None (Part-2, Page-31, 90)
FAU_SAA.1	Security Audit Analysis	1) Enabling and disabling of any of the analysis mechanisms 2) Automated responses performed by the tool.
FAU_STG.1	Security Audit event Storage	None
FDP_IFC.1	Information Flow Control policy	None
FIA_ATD.1	User Attribute definition	None
FIA_AFL.1	User Attribute definition	1) Consecutive 3 unsuccessful use of the authentication mechanism for the same user (except Administrator) 2) Re-enabling of a locked account by Administrator
FIA_SOS.1	Specification of Secrets	Rejection by the TSF of any tested secret
FIA_UAU.2 FIA_UAU.5	User Authentication	Unsuccessful use of the authentication mechanism
FIA_UID.2	User Identification	Unsuccessful use of the user identification mechanism, including the user identity provided
FMT_MSA.3	Management of	1) Modifications of the

	Security attributes	default setting of permissive or restrictive rules. 2) All modifications of the initial values of security attribute
FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c FMT_MTD.1d FMT_MTD.1e	Management of TSF data	1) All modifications to the router configuration 2) User attribute modification 3) Deletion of Audit logs 4) Change of time configuration
FMT_SMR.1	Security Management Roles	modifications to the group of users that are part of a role;
FMT_SMF.1	Specification of Management functions	Use of the management functions.
FPT_STM.1	Time stamps	changes to the time;
FPT_TST_EXT.1	Extended component	None
FPT_RCV.1	Trusted recovery	1) The fact that a failure or service discontinuity occurred; 2) resumption of the regular operation;
FPT_FLS.1	Fail Secure	1) Controller card switchover; 2) Process termination
FPT_DSP_EXT.1	Extended component.	None
FTA_MCS.1	TOE session establishment	Denial of a session establishment due to maximum number of concurrent sessions is

		reached
FTA_SSL.3	Session termination on inactivity	Termination of a session due to user inactivity

FAU_GEN.1.2

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

Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [no additional information].

6.2.1.3 User identity association (FAU_GEN.2)

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.

6.2.1.4 Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;

b) [No other events].

6.2.1.5 Audit review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide [Restricted-operator, Operator, Restricted-admin, Administrator] with the capability to read [all information] from the audit records

FAU_SAR.1.2

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

6.2.1.6 Protected audit trail storage (FAU_STG.1)

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.

6.2.2 User data protection (FDP)

6.2.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] on

a [subjects:
- Unauthenticated external IT entities that send and receive packets through the TOE to one another;

b information (packets):
- Network packets sent through the TOE from one subject to another;

c operation:

- Route packets].

6.2.2.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] based on the following types of subject and information security attributes: [

a subject security attributes:

- Presumed address

b information security attributes:

- Presumed address of source subject
- Presumed address of destination subject
- Network layer protocol
- TOE interface on which packet arrives and departs

]

FDP_IFF.1.2

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

a [subjects on a network can cause packets to flow through the TOE to another connected network if:

all the packet security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the packet security attributes, created by the authorized user;

the presumed address of the source subject, in the packet, is consistent with the network interface it arrives on;

and the presumed address of the destination subject, in the packet, can be mapped to a configured nexthop].

FDP_IFF.1.3

The TSF shall enforce the [no additional UNAUTHENTICATED SFP rules].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules that explicitly authorize information flows].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [no additional rules that explicitly deny information flows].

6.2.3 Identification and authentication (FIA)

6.2.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

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

a User identity;

b Authentication data;

c Privileges].

6.2.3.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [password – Alphanumeric string of length minimum 8 characters excluding control characters].

6.2.3.3 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1

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

6.2.3.4 User identification before any action (FIA_UID.2)

FIA_UID.2.1

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

6.2.3.5 Authentication failure (FIA_AFL.1)

FIA_AFL.1.1

The TSF shall detect when [3] unsuccessful authentication events occur related to [login of users except Administrator].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [lock the account until the authentication administrator re-enables it].

6.2.3.6 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1

The TSF shall provide [internal password mechanism, SSH public key and external server (RADIUS or TACACS) mechanism] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by Administrator].

6.2.4 Security management (FMT)

6.2.4.1 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the [UNAUTHENTICATED SFP] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [Restricted-admin and Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.2 Management of TSF data (Router/Switch configuration) (FMT_MTD.1a)

FMT_MTD.1.1a

The TSF shall restrict the ability to [modify] the [router configuration data] to [Restricted-admin, Administrators].

6.2.4.3 Management of TSF data (User attributes) (FMT_MTD.1b)

FMT_MTD.1.1b

The TSF shall restrict the ability to [modify] the [user account attributes] to [Administrators].

6.2.4.4 Management of TSF data (Audit logs) (FMT_MTD.1c)

FMT_MTD.1.1c

The TSF shall restrict the ability to [delete] the [audit logs] to [Administrators].

6.2.4.5 Management of TSF data (Date/time) (FMT_MTD.1d)

FMT_MTD.1.1d

The TSF shall restrict the ability to [modify] the [NTP Server address] to [Restricted-admin, Administrator].

6.2.4.6 Management of TSF data (Sessions) (FMT_MTD.1e)

FMT_MTD.1.1e

The TSF shall restrict the ability to [modify] the [rules that restrict the ability to establish management sessions] to [Restricted-admin and Administrator].

6.2.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the privilege levels to differentiate [Non-privileged user, Restricted-operator, Operator, Restricted-admin, Administrator]

The TSF supports 5 types of user levels as described below:

Table 6 User Levels

User role[1]	Privilege Level	Operations
Non-privileged user	0 - 2	• Escalate own privilege by “enable” command if permitted
Restricted-Operator	3 - 6	• Show commands
Operator	7 - 9	All actions as Restricted-Operator + • Enter Exec mode (though can not perform anything in that mode, further functionality will be available in future releases)

Restricted-Admin	10 - 14	All actions as operator + • Change configuration • Rename files
Administrator	15	All actions of Restricted-Admin + • Change User Attributes • Create Another Administrator • Copy/edit/delete Files

[1] User roles are classified logically – as per their functions / privilege and do not reflect in the config file

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.4.8 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

- Configuring Management Access
- Configuring IP ACL Filters
- Configuring Login control (authentication method to use: local/radius, ssh server attributes etc.)
- Configuring RADIUS/TACACS
- Configuring SNMP/ Syslog
- Configuring NTP

All these functions can be carried out by Restricted-Admin or Administrator

- Configuring Administrators;
- Configuring user attributes;
- Copying and Overwriting Administrators and user attributes;

The above functions can be performed only by Administrator.

6.2.5 Protection of the TOE security functions (FPT)

6.2.5.1 Time stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.2.5.2 Self Test (FPT_TST_EXT.1)

FPT_TST_EXT.1.1

The TSF shall run a suite of self tests [*during initial start-up*] to demonstrate the correct operation of [*parts of the TSF as below*].

- TSF configuration management binary
- Command line interface binary
- Data-plane management binaries

6.2.5.3 Fail Secure (FPT_RCV.1)

FPT_RCV.1.1

The TSF should be able to provide a trusted recovery.

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

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [

- Controller card failure (applicable for models SE600, SE1200, SE1200H only, since SE100 has only one controller card a hardware failure can't be recovered by switchover to standby one)
- Process termination]

6.2.5.5 Domain separation – data and Mgmt (FPT_DSP_EXT.1)

FPT_DSP_EXT.1

The TSF should be able to provide a domain separation between data plane and management plane.

6.2.6 TOE access (FTA)

6.2.6.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions that belongs to the same user.

FTA_MCS.1.2

The TSF shall enforce by default, a limit of [10 total maximum number of sessions per user who is not Administrator, which is configurable up to 32, and 1 for Administrator].

6.2.6.2 Session Termination on Inactivity (FTA_SSL.3)

FTA_SSL.3.1

The TSF shall terminate an interactive session after [10 minutes of user inactivity].

6.2.6.3 TOE session establishment (FTA_TSE.1)

FTA_TSE.1

The TSF shall be able to deny session establishment based on [presumed origin of the request].

6.2.7 Cryptographic Support (FCS)

FCS_CKM.1

Cryptographic Key Generation - DSA (Digital Signature Algorithm), DH (Diffie-Hellman exchange)

FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [DSA] and specified cryptographic key size [1024] bits that meets the following: [PKCS #1].

The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [DH group1, DH group14] and specified cryptographic key sizes [1024, 2048] bits that meets the following: [RFC 4253].

FCS_CKM.4

Cryptographic key Destruction

FCS_CKM.4.1

The TSF shall destroy asymmetric cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following [none].

The TSF shall destroy symmetric cryptographic keys in accordance with a specified cryptographic key destruction method [delete] that meets the following [none].

FCS_COP.1

Crypto Operation - Remote Administration by SSH

FCS_COP.1.1

The TSF shall perform encryption of [remote authorized user sessions] in accordance with a specified cryptographic algorithm [for host key exchange: Digital Signature Standard as specified in FIPS PUB 186-3 with key length 1024 bits; for symmetric encryption: Triple Data Encryption Standard (3DES) as specified in FIPS PUB 46-3 with keying option 1; or Advanced Encryption Standard (AES) as specified in FIPS PUB 197 with key lengths of 128, 192 or 256 bits; for user authentication: Digital Signature Algorithm (DSA) as specified in FIPS PUB 186-3] that meet the following [FIPS PUB 46-3].

6.3 Security Assurance Requirements

The following table describes the TOE security assurance requirements drawn from Part 3 of the CC.

Table 7 Security Assurance Requirements

Assurance Class	Assurance Components

Security Target (ASE)	*ST introduction (ASE_INT.1)*
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	*Security architecture description (ADV_ARC.1)*
	Functional specification with complete summary (ADV_FSP.3)
	Architectural design (ADV_TDS.2)
Guidance documents (AGD)	*Operational user guidance (AGD_OPE.1)*
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	*Authorization controls (ALC_CMC.3)*
	Implementation representation CM coverage (ALC_CMS.3)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	*Vulnerability analysis (AVA_VAN.2)*

7 TOE Summary Specification

7.1 TOE Security Functions

7.1.1 Information Flow Function

FDP_IFC.1 Subset information flow control and FDP_IFF.1 Simple security attributes

The TOE is designed primarily to route unauthenticated network traffic. Network traffic represents information flows between source and destination network entities. The specific routing of traffic is based on the routing configuration data that has been created by the TOE users or has been collected (e.g., ARP, BGP) from network peers as defined by the TOE users. The routing decision is based on the presumed source and destination IP address of the packet, the network layer protocol, service and the interface on which the packet arrives and is to depart on.

7.1.2 Identification and Authentication Function

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name, authentication data (password, public key) and privilege (user class). The Administrator can delegate the authentication process to a RADIUS or TACACS server.

If a user is authenticated remotely, a template user account on the TOE may be used to determine the privileges, rather than specifying privileges for each user. In this instance, a template user account is configured on the TOE and an individual user account is configured on the external authentication server. When the authentication server successfully authenticates the user they pass the unique username and the template account the username is to be associated is passed to the TOE. The user name that was authenticated is used when generating audit records regarding activity by that user.

FIA_SOS.1 Verification of secrets

Locally stored authentication data for password authentication is a case−sensitive, alphanumeric value. The password is an alphanumeric string excluding control characters having a minimum length of 8 characters. This password is digested in the configuration repository.

FIA_UAU.2 User authentication before any action, FIA_UAU.5 Multiple authentication mechanisms and **FIA_UID.2 User identification before any action**

The TOE requires users to provide unique identification and authentication data (passwords or in case of SSH public key) before any administrative access to the system is granted.

The SEOS software supports four methods of user authentication: local password authentication, local authentication using public key authentication (via the SSH application), Remote Authentication Dial - In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS).

With local password authentication, a password is configured for each user allowed to log into the Services Router/switch. RADIUS and TACACS are authentication methods for validating users who attempt to access the router. Both are distributed client/server systems—the RADIUS and TACACS clients run on the appliance, and the server runs on a remote network system in the IT environment.

If the identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternately, if the TOE is configured to work with a RADIUS or TACACS server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until successful authentication as an authorized administrator.

It should be noted that when RADIUS and/or TACACS are used for authentication, the TOE can verify only that the remote authentication server has the correct credentials.

The TOE can be configured to allow users to be authenticated via RADIUS and/or TACACS. The order in which authentication mechanisms are attempted is applied to all users. The configuration can also specify that local passwords can only be used when external authentication servers are unavailable, or as a general fallback. If configured and the request is made via SSH, public key authentication will be the attempted first; this is hard coded and is not specified in the authentication order.

Local authentication using the SSH application utilizes the user's public key stored on the appliance to both establish the SSH session and to authenticate the user to the CLI.

Irrespective of what access method is used for management sessions, successful authentication is required prior to giving a user access to the system. These mechanisms are used for administration of the routing functions as well as the administration of the user accounts used for management.

Authentication data can be stored either locally or on a separate server. The separate server must support either the RADIUS or TACACS protocols to be supported by the TOE.

FIA_AFL.1 Authentication failure

After 3 consecutive login failures for a particular user, the account will be locked and only Administrator can unlock the account.

7.1.3 Security Management Function

The TOE restricts to Administrator the ability to enable, disable or modify the behavior of generating and sending authentication requests and related records.

Mechanism which makes it possible to achieve this is due to every user account having associated with the privilege level and every action of the user could be authorized through sending authorization request to local or external AAA servers & obtaining the authorization information for the user, and only after successful authorization of the privilege level associated with the user, execution of enabling or disabling or to modify any configurations (these configuration could even be the controlling of how authentication or authorization and auditing itself is done in done by the TOE), towards managing security functions.

The TOE restricts to Administrator the ability to add or delete users, modify their access permissions or manage authentication attributes.

The management functions are as follows:
- Configuring Management Access;
- Configuring IP ACL Filters;
- Configuring Administrators;
- Configuring user attributes;
- Copying and Overwriting Administrators and user attributes;
- Configuring Login control;
- Configuring RADIUS/TACACS;
- Configuring SNMP/Syslog;
- Configuring NTP;

FMT_MSA.3 Static attribute initialization

As default, the TOE allows SSH connection and prevents all other types of network connections through the TOE if a rule has been set up to allow the type of communication to pass.

FMT_MTD.1a Management of TSF Data (Router/Switch Information)

The TOE restricts the ability to administer the router configuration data. The CLI provides a text - based interface from which the router configuration can be managed and maintained. From this interface all TOE functions, such as BGP, RIP and MPLS protocols can be managed, as well as TCP/IP configurations and date/time. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

FMT_MTD.1b Management of TSF Data (User Data)

The TOE restricts the ability to administer user data to only Administrators. The CLI provides admin - users with a text - based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted. This interface also provides the Administrator with the ability to configure an external authentication server, such as a RADIUS or TACACS server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE. If authentication - order includes RADIUS and/or TACACS, then these will be consulted in the configured order for all users. Typically, local password is only used as a fallback in such cases.

FMT_MTD.1c Management of TSF Data (Audit logs)

The TOE can be configured to automatically delete audit logs, or they can be deleted manually.

FMT_MTD.1d Management of TSF Data (Date/time)

The TOE will allow only a Restricted-admin or Administrator to modify the date/time setting on the appliance.

FMT_MTD.1e Management of TSF Data (Sessions)

The TOE will allow only a Restricted-admin or Administrator to create, delete or modify the rules that control the presumed address from which management sessions can be established.

FMT_SMF.1 Management of Security Functions

The TOE provides the ability to manage the following security functions:

User authentication (authentication data, roles);

TOE information;

Audit management and review;

Modify the time;

Session establishment restrictions.

FMT_SMR.1 Security Roles

The TOE has privilege levels defined per user. When a new user account is created, it must be assigned one of the privilege levels.

- Administrator (privilege level 15): User with this privilege level can perform all management functions on the TOE. A user with this role can manage user accounts (create, delete, modify), view and modify the TOE configuration information.
- Restricted-admin (privilege level 10 to 14): User with this privilege level can read some configuration data, and in addition can use the following commands:

  Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands),

  Can access the network by entering the ping, SSH and traceroute commands,

  Can restart software processes using the restart command.

  Can view trace file settings in configuration and operational modes.

  Can review all audit records.
- Operator (privilege level 7 to 9): Can view all configurations, can enter exec mode
- Restricted-operator (privilege level 3 to 6): Can view all configuration
- Non-privileged user (privilege level 0 to 2): None.

7.1.4 Audit Function

FAU_GEN.1 Audit data generation

SEOS creates and stores audit records for the following events:
- Start - up and shutdown of the audit function;
- User login/logout;
- Login failures;
- Configuration is committed;
- Configuration is changed.

Auditing is done using syslog. This can be configured to store the audit logs locally, or to send them to one or more log servers. The syslogs are automatically deleted locally according to configurable limits on storage volume or number of days of logs to retain.

FAU_GEN.2 User identity association

SEOS will record within each audit record the following information:

Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and Identity of the user causing the event.

FAU_SAR.1 Audit review

SEOS provides Restricted-operator, Operator, Restricted-admin, Administrator users with the ability to display audit data from the CLI. Commands are available to list entire files, or to select records that match or do not match a pattern. Records can also be saved to files for further analysis offline. Read only users cannot view the audit records.

FAU_STG.1 Protected audit trail storage

Audit records are stored in files. Both the files and that directory are only modifiable by the Administrators.

FAU_ARP.1 Security alarms

The daemons that authenticate the users if notices 3 successive login failures will generate an audit log message.

FAU_SAA.1 Potential violation analysis

The daemons authenticating users to SEOS perform analysis of the failed authentication attempts to identify activity indicating a potential violation. The following patterns of activity are defined to represent a potential violation and the action specified is triggered:

After 3 successive login failures, the connection will be dropped.

The TOE can also be configured to display selected audit events as they occur.

7.1.5 TOE Access Function

FTA_TSE.1 TOE session establishment

The TOE can be configured by a Restricted-admin or Administrator through use of packet filters such that users can only gain access from specific management networks/stations at specific IP addresses.

FTA_MCS.1 Maximum number of concurrent sessions

The TOE allows a maximum of 10 concurrent sessions for every user by default, which is configurable up to 32 for who are not Administrator, and a single session for Administrator.

FTA_SSL.3 Session termination on user inactivity

The TOE will terminate a session after 10 minutes of inactivity.

7.1.6 Clock function

FPT_STM.1 Time stamps

The clock function of the TOE provides a source of date and time information for the appliance, used in audit timestamps. The clock function is reliant on the system clock provided by the underlying hardware.

For better accuracy of timestamp and synchronization of time across devices in the IT environment, an external NTP server can be deployed. In such deployments the audit timestamps will be synchronized with external syslog servers, if configured

7.1.7 TOE self test

FPT_TST.1 Self Test

The TOE consists of a set of daemons, which implement the functions such as – AAA, routing protocols etc. These daemons are invoked by the process manager. The process Manager checks the integrity of the daemon binaries, before starting them up.

7.1.8 Trusted Recovery

FPT_RCV.1 Trusted Recovery

The TOE high availability and process restorability are used for trusted recovery across processes and version upgrades.

7.1.9 Fail Secure

FPT_FLS.1 Failure with preservation of secure state

When there are switchovers such as XCRP switchover, the TOE recovers the current running state. There are a many hardware and software features that promote high availability and redundancy:

- Redundant Hot standby XCRP controller card with hitless fail over and no interruption to traffic forwarding, subscriber sessions and L2TP tunnels
- When one of the processes get killed, the system automatically detects the condition and restarts the process
- When the SEOS boots up, system checks for the integrity of the daemon and prevents the boot up if the integrity check fails

7.1.10 Domain separation

FPT_DSP_EXT.1 TSF domain separation

The TOE offers clear separation of data and control/management plane at its architecture.

7.1.11 Protection of the TSF

The TOE implements secure shell (SSH) as a remote access mechanism using DSA key generation and 168 bit 3DES or 128, 192 or 256 bits AES encryption. This protects all the exchanges between the TOE and the remote management client from reading or modification by any other entity in the network. Remote management via SSH provides access to the management CLI. When new cryptographic keys are generated, the old ones are overwritten.

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
- Dependencies

8.1 Rationale for Security Objectives

This section shows that all assumptions and threats are countered by security objectives, and that each security objective addresses at least one assumption or threat.

8.1.1 Rationale for Security Objectives for the TOE

This section provides a mapping of TOE security objectives to those threats that the TOE is intended to counter, and to those assumptions that must be met.

Table 8 TOE Security Objectives Rationale

	T.ROUTE	T.PRIVIL	T.INTERCEPT	T.CONFLOSS	T.NOAUDIT	T.PROTECT
O.FLOW	✓					
O.ACCESS		✓				
O.ENCRYPT			✓			
O.ROLBAK				✓		
O.AUDIT					✓	

O.PROTECT						✓

O.FLOW: This objective helps to counters the threat T.ROUTE through the use of routing tables to correctly route information.

O.ACCESS: This objective addresses the need to protect the TOE's operations and data against unauthorized access (T.PRIVIL)

O.ENCRYPT: This objective address the need to prevent the interception of the remote management data by encrypting the remote management data (T.INTERCEPT)

O.ROLBAK: The objective to restore previous configurations helps recover from loss of configuration data (T.CONFLOSS)

O.AUDIT: This objective serves to discourage and detect inappropriate use of the TOE (T.NOAUDIT)

O-PROTECT: This objective is to prevent unauthorized users from gaining accessing to the TOE's configuration data (T.PROTECT)

8.1.2 Rationale for Security Objectives for the Environment

This section provides a mapping of environment security objectives to those threats that the environment is expected to counter, and to those assumptions that must be met.

Table 9 Environment Security Objectives Rationale

	A.LOCATE	**A.NOEVIL**	**A.TIME**	**A.EAUTH**
OE.PHYSICAL	✓			
OE.ADMIN		✓		
OE.TIME			✓	

OE.EAUTH				✓

OE.EAUTH: The objective to have a AAA server (RADIUS / TACACS) in the TOE environment for external Authentication, Authorization and Accounting (A.EAUTH).

OE.TIME: The objective to have an NTP server in the TOE environment supports the assumption (A.TIME) that time services are available to provide the appliance with accurate/synchronized time information.

OE.PHYSICAL: The objective to provide physical protection for the TOE supports the assumption that the TOE will prevent unauthorized physical access (A.LOCATE).

OE.ADMIN: The objective that users should follow administrator guidance supports the assumption that they will not be careless, willfully negligent or hostile (A.NOEVIL).

8.2 Rationale for Security Requirements

8.2.1 Rationale for TOE Security Functional Requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and that each security functional requirement for the TOE addresses at least one security objective for the TOE. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 8 and Table 9 demonstrate the relationship between the threats and assumptions and the security objectives. Table 10 illustrates the mapping between security functional requirements and security objectives for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

Table 10 Security Functional Requirements Rationale

	O.FLOW	O.ACCESS	O.ROLBAK	O.AUDIT	O.ENCRYPT	O.PROTECT
FAU_ARP.1				✓		
FAU_GEN.1				✓		
FAU_GEN.2				✓		
FAU_SAA.1				✓		
FAU_SAR.1				✓		
FAU_STG.1				✓		
FDP_IFC.1	✓					
FDP_IFF.1	✓					
FIA_ATD.1		✓		✓		
FIA_SOS.1		✓				
FIA_AFL.1		✓				
FIA_UAU.2		✓				
FIA_UAU.5		✓				
FIA_UID.2		✓				

	O.FLOW	O.ACCESS	O.ROLBAK	O.AUDIT	O.ENCRYPT	O.PROTECT
FMT_MSA.3		✓				
FMT_MTD.1a	✓					
FMT_MTD.1b		✓				
FMT_MTD.1c				✓		
FMT_MTD.1d				✓		
FMT_MTD.1e		✓				
FMT_SMF.1		✓		✓		
FMT_SMR.1		✓		✓		
FPT_STM.1				✓		
FTA_TSE.1		✓				
FTA_MCS.1		✓				
FTA_SSL.3		✓				
FPT_RCV.1						✓
FPT_FLS.1			✓			✓
FPT_DSP_EXT.1						✓

	O.FLOW	O.ACCESS	O.ROLBAK	O.AUDIT	O.ENCRYPT	O.PROTECT
FCS_CKM.1					✓	
FCS_CKM.4					✓	
FCS_COP.1					✓	
FPT_TST_EXT.1						✓

FAU_ARP.1 This component takes action following detection of potential security violations, and therefore contributes to meeting O.AUDIT.

FAU_GEN.1 This component outlines what events must be audited, and aids in meeting O.AUDIT.

FAU_GEN.2 This component required that each audit event be associated with a user, and aids in meeting O.AUDIT.

FAU_SAA.1 This component helps to detect potential security violations, and aids in meeting O.AUDIT.

FAU_SAR.1 This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_STG.1 This component requires that unauthorized deletion of audit records does not occur, and thus helps to maintain accountability for actions, as required by O.AUDIT.

FDP_IFC.1 This component identifies the entities involved in the UNAUTHENTICATED information flow SFP (i.e. external IT entities sending packets), and aids in meeting O.FLOW.

FDP_IFF.1 This component identifies the conditions under which information is permitted to flow between entities (the UNAUTHENTICATED SFP), and aids in meeting O.FLOW.

FIA_ATD.1 This component specifies that individual user attributes to be maintained and aids in meeting O.ACCESS and O.AUDIT.

FIA_AFL.1 This component protects against repeated unauthorized access attempts and hence helps meeting O.ACCESS.

FIA_SOS.1 This component specifies metrics for authentication, and aids in meeting objectives to restrict access O.ACCESS

FIA_UAU.2 This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access and aids in meeting O.ACCESS

FIA_UAU.5 This component was selected to ensure that appropriate authentication mechanisms can be selected. As such it aids in meeting objectives to restrict access O.ACCESS.

FIA_UID.2 This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access O.ACCESS.

FMT_MSA.3 This component ensures that there is a default deny policy for the information flow control security rules. As such it aids in meeting O.ACCESS.

FMT_MTD.1a This component restricts the ability to modify routing configuration details, and as such aids in meeting O.FLOW.

FMT_MTD.1b This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.ACCESS.

FMT_MTD.1c This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT.

FMT_MTD.1d This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT.

FMT_MTD.1e This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.ACCESS.

FMT_SMF.1 This component lists the security management functions that must be controlled. As such it aids in meeting O.ACCESS and O.AUDIT.

FMT_SMR.1 Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting, O.ACCESS and O.AUDIT.

FPT_STM.1 This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.

FPT_RCV.1 This component ensures that reliable recovery mechanism is performed in meeting O.PROTECT

FPT_FLS.1 This component ensures that reliable recovery is performed under certain hardware and software failures and helps meeting O.PROTECT. It also helps in rolling back to a previously saved configuration thus helping meet the O.ROLBACK objective.

FPT_DSP_EXT.1 This component ensures that clear separation of data and management plane are available and aids in meeting O.PROTECT

FTA_TSE.1 This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS.

FTA_MCS.1 This component limits the number of sessions a user can establish, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS.

FTA_SSL.3 This self-terminates idle sessions after a timeout, and hence reduces the chances of unauthorized access via unattended sessions. This helps meeting O.ACCESS.

FCS_CKM.1 & FCS_CKM.4 Defines cryptographic key management functions, namely the generation and destruction of keys. These key management secures the cryptographic operations and hence meets objective O.ENCRYPT

FCS_COP.1 is the actual cryptographic operation that secures the communication between the TOE and users, meeting the objective O.ENCRYPT

FPT_TST_EXT.1 This component ensures that reliable self test are performed and aids in meeting O.PROTECT

8.3 Rationale for Security Assurance Requirements (SAR)

The TOE meets the independent security assurance requirements of ISO-15408.

8.3.1 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC2] and [CC3] have been satisfied, with the exception of the dependency of FMT_MSA.3 on FMT_MSA.1. The requirement for FMT_MSA.3 is included as a dependency from FDP_IFF.1, to specify how the security attributes associated with the information flow rules are initialized. The subsequent dependency from FMT_MSA.3 on FMT_MSA.1 allows for the specification of the management of the security attributes. However, for this TOE the management of the information flow security attributes is specified using FMT_MTD.1a. Therefore, there is no need to include FMT_MSA.1 as FMT_MTD.1a has satisfied the intent of the dependency.

No additional dependencies have been identified. Dependencies on FIA_UAU.1 and FIA_UID.1 have been satisfied through inclusion of the hierarchical components FIA_UAU.2 and FIA_UID.2, respectively.

FAU_GEN.2 is dependent on FIA_UID.1, which is satisfied through inclusion of the hierarchical component FIA_UID.2

9 Acronyms

Table 11 Acronyms

AAA	Authentication Authorization Auditing
ACM	Access Control Management
AGD	Administrator Guidance Document
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BSD	Berkley Software Distribution
CC	Common Criteria
CD	ROM Compact Disk Read Only Memory
CLI	Command Line Interface
CM	Control Management
DAC	Discretionary Access Control
DPC	Dense Port Concentrators
EAL	Evaluation Assurance Level
EPPA	Egress Packet Processing ASIC
GB	Gigabyte
I/O	Input/Output
IPPA	Ingress Packet Processing ASIC
IS-IS	Intermediate System to Intermediate System
NPM	Network Policy Manager
OSPF	Open Shortest Path First
PFE	Packet Forwarding Engine
PIC	Pluggable Interface Controller
PIM	Protocol Independent Multicast
PMA	Packet Mesh ASIC
PP	Protection Profile

RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TACACS	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
XFP	Optical Transceiver