Alcatel-Lucent Service Router Operating System (SR OS) v7.0 Security Target

Document No. 1607-001-D000
Version v1.8, 6 April 2010

Prepared for:
Alcatel-Lucent
701 East Middlefield Road
Mountain View, CA
USA, 94043

Prepared by:
Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 SECURITY TARGET (ST) INTRODUCTION

1.1 ST PURPOSE

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Service Router Operating System (SR OS) v7.0, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the SR OS satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.2 ST REFERENCE

1.2.1 ST Title:

Alcatel-Lucent Service Router Operating System (SR OS) v7.0 Security Target.

1.2.2 ST Version Number:

Version v1.8

1.2.3 ST Publication Date:

6 April 2010

1.2.4 ST Authors:

Electronic Warfare Associates-Canada, Ltd. (EWA-Canada)

1.2.5 Conventions

1.2.5.1 Operations

The CC permits four types of operations to be performed on security functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

a. Selection: Indicated by surrounding brackets and italicised text, e.g., [*selected item*].
b. Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item].
c. Refinement: Indicated by underlined text, e.g., refined item for additions or strikethrough text, e.g., ~~refined item~~ for deleted items.
d. Iteration: Indicated by assigning a number at the functional component level, for example:
   FDP_IFF.1(1) Simple security attributes (unauthenticated policy);
   FDP_IFF.1(2) Simple security attributes (authenticated policy); and
   FDP_IFF.1(3) Simple security attributes (export policy).

The markings are relative to the requirement statements in the CC.

1.2.6 CC Acronyms, Abbreviations and Initializations

Acronyms and Abbreviations

ADV	Assurance Development
AGD	Assurance Guidance Documents
ALC	Assurance Life-Cycle
ASE	Assurance Security Target Evaluation
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Evaluation Methodology
CSEC	Communications Security Establishment Canada
DES	Description
DOS	Denial of Service
EAL	Evaluation Assurance Level
EAL 2+	Evaluation Assurance Level 2+
INT	Introduction
IT	Information Technology
OBJ	Security Objectives
OSP	Organizational security policies
REQ	IT Security Requirements
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

1.2.7 Product/TOE Terminology

The following terms are listed here to aid the reader of the ST:

7x50	-	A collective term used in this document to refer to both the 7750 SR and 7450 ESS.
77x0	-	A collective term used in this document to refer to both the 7710 and 7750 SR.
ACL	Access Control List	It is filter policy applied on ingress or egress to a service SAP on an interface to control the traffic access.
ATM	Asynchronous Transfer Mode	ATM is a standardized digital data transmission technology. ATM is a cell-based switching technique that uses asynchronous time division multiplexing.
BGP	Border Gate Protocol	The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rulesets.
CIR	Committed Information Rate	CIR is the amount of bandwidth that the carrier is committed to provide to the subscriber.
CLI	Command Line Interface	A text based administrator interface to configure a 7x50 node.
CPE	Customer Premise Equipment	Equipment that is installed in customer premises by a service provider to connect to a specific service.
CPM	Control Processor Module	Module within the SR/ESS.
CPM filter	CPM filter	SR/ESS-Series routers with separate CPM modules (7710 SR-c4 and SR-c12, 7750 SR-7 and SR-12, and ESS-6, ESS-7 and ESS-12i models), have traffic management and queuing hardware on the CPM modules dedicated to protecting the control plane. CPM filters can be created on this hardware. These filters can be used to drop or accept packets, as well as allocate dedicated hardware shaping queues for traffic directed to the control processors.

CPMQ	Control Processor Module Queuing	Control Processor Module Queuing (CPMQ) implements separate hardware-based CPM queues which are allocated on a per-peer basis. Administrators can allocate dedicated CPM hardware queues for certain traffic designated to the CPUs and can set the corresponding rate-limit for the queues.
CPU	Central Processing Unit	All traffic destined to the CPM and that will be processed by its CPU
DUSA	Documented Special Use Addresses	Documented Special Use IPv4 addresses
ESS	Ethernet Service Switch	ESS-Series router
FR	Frame Relay	A data transmission technique that combines high-speed and low-delay circuit switching with the port sharing and dynamic bandwidth allocation capabilities of X.25 packet switching. Like X.25, frame relay divides transmission bandwidth into numerous virtual circuits and implements bursts of data. But unlike X.25, frame relay does not require a lot of processing at each node, delegating error correction and flow control to the attached devices.
GRE	Generic Routing Encapsulation	GRE is a tunnelling protocol. Using GRE packets that belong to a wide variety of protocol types are encapsulated inside IP tunnels, which creates a point-to-point link over an IP network.
IB	In-band	Interfaces using a physical I/O port on the router.
IETF	Internet Engineering Task Force	The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standards bodies and dealing in particular with standards of the TCP/IP and Internet protocol suite. It is an open standards organization.
IOM	Input Output Module	SR/ESS modules that interconnects two MDAs with fabric core. The module also performs Layer 3 traffic management. Part of Data Pane.
IP	Internet Protocol	A network layer protocol underlying the Internet, which provides an unreliable, connectionless, packet delivery service. IP allows large, geographically-diverse networks of computers to communicate with each other quickly and economically over a variety of physical links.
IS-IS	Intermediate system to intermediate system	Intermediate system to intermediate system (IS-IS), is a protocol used by network devices (routers) to determine the best way to forward datagrams through a packet-switched network, a process called routing.

LAG	Link Aggregation Group	Based on the IEEE 802.3ad standard, LAGs are configured to increase the bandwidth available between two network devices. All physical links in a given LAG combine to form one logical interface.
LAN	Local Area Network	A system designed to interconnect computing devices over a restricted geographical area (usually a couple of kilometres)
LDP	Label Distribution Protocol	LDP (Label Distribution Protocol) is a new protocol that defines a set of procedures and messages by which one LSR (Label Switched Router) informs another of the label bindings it has made.
LSP	Label Switched Path	A sequence of hops in which a packet travels by label switching.
LSR	Label Switch Router	A node capable of forwarding datagrams based on a label.
MAC	Media Access Control	A media-specific access control protocol within IEEE802 specifications. The protocol is for medium sharing, packet formatting, addressing, and error detection.
MBS	Maximum Burst Size	One of the parameters associated with queue configuration in 7x50. This is the maximum buffer space available for the traffic flows associated with the queue.
MAF	Management Access Filter	Management access filters control all traffic in and out of the CPM. They can be used to restrict management of the SR/ESS-Series router by other nodes outside either specific (sub)networks or through designated ports.
MDA	Media Dependant Adapter	MDAs are modules that are housed in IOMs and in which a physical interface terminates.
MIB	Management Information Base	A MIB is a type of database used for managing the devices in a communications network.
MPLS	Multi-Protocol Label Switching	MPLS technology implements the delivery of highly scalable, differentiated, end-to-end IP and VPN services. The technology allows core network routers to operate at higher speeds without examining each packet in detail, and allows differentiated services.
MSDP	Multicast Source Discovery Protocol	MSDP is a computer network protocol in the Protocol Independent Multicast (PIM) family of multicast routing protocols.
OOB	Out-of-band	Refers to the RS-232 Console port or the management Ethernet port on the SR.

OSPF	Open Shortest Path First	A link-state routing algorithm that is used to calculate routes based on the number of routers, transmission speed, delays and route cost.
RADIUS	Remote Authentication Dial-In User Service	A client/server security protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize access to the requested system or service.
RFC	Request for Comments	An Internet Engineering Task Force (IETF) memorandum on Internet systems and standards
RIP	Routing Information Protocol	RIP is based on distance-vector algorithms that measure the shortest path between two points on a network, based on the addresses of the originating and destination devices. The shortest path is determined by the number of “hops” between these points. Each router maintains a routing table, or routing database, of known addresses and routes; each router periodically broadcasts the contents of its table to neighbouring routers in order that the entire network maintain a synchronised database.
RTM	Route Table Manager	The RTM controls the configuration of the routing table which stores the routes (and in some cases, metrics associated with those routes) to particular network destinations.
QoS	Quality of Service	A set of performance parameters that characterize the traffic over a given connection
SAM	Service Aware Manager	Provides GUI management functions (e.g., provisioning) for the 7710, 7750 & 7450. The SAM is defined outside the TOE boundary with a Console CLI (provides administrators with backside services) also outside the TOE boundary. Both the 7710/7750 SR and the 7450 ESS can be managed by the 5620 SAM. The SAM includes the Element Manager (SAM-E), Provisioning (SAM-P), and Assurance (SAM-A) modules. The operational environment requires a RADIUS or TACACS+ server for authentication/authorization services, the SAM for limited remote administration, local Console access for most administration, SNMP/Syslog servers for logging, and a Network Time Protocol (NTP) server for external time synchronization
SAP	Service Access Point	A SAP identifies the customer interface point for a service on a SR/ESS.

SDH	Synchronous Digital Hierarchy	Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs).
SONET	Synchronous optical networking	Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs).
SR	Service Router	SR-Series router
SR/ESS	Service Router/ Ethernet Service Switch	A collective term used in this document to refer 7710 SR, 7750 SR and 7450 ESS.
SR OS	Service Router Operating System	The TOE consisting of the Alcatel-Lucent Service Router Operating System (SR OS) which is an integral component of the Alcatel-Lucent service router product family, which includes the: • Alcatel-Lucent 7710 Service Router (SR) (models SR-c4, SR-c12) • Alcatel-Lucent 7750 Service Router (SR) (models SR-1, SR-7 and SR-12) • Alcatel-Lucent 7450 Ethernet Service Switch (ESS) (models ESS-1, ESS-6, ESS-7 and ESS-12. The hardware for the above listed models is excluded from the TOE boundary, with the exception of the CPM hardware queue for SR/ESS-Series routers with separate CPM modules (7710 SR-c4 and SR-c12, 7750 SR-7 and SR-12, and ESS-6, ESS-7 and ESS-12i models).
TCP	Transmission Control Protocol	TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
TTL	Time to Live	TTL is a limit on the period of time or number of iterations or transmissions in computer and computer network technology that a unit of data (e.g. a packet) experiences before it should be discarded
TACACS +	Terminal Access Controller Access Control System Plus	An authentication protocol that allows a remote access server to forward an administrator's logon password to an authentication server to determine whether access is allowed to a given system.

UDP	User Datagram Protocol	UDP is transport layer protocol which do not guarantee delivery of data
UTC	Universal Time Coordinated	Time zones around the world can be expressed as positive or negative offsets from UTC; UTC has replaced GMT as the basis for the main reference time scale. UTC is derived from International Atomic Time (TAI).
VPN	Virtual Private Network	A way to provide secure and dedicated communications between a group of private servers over public Internet.
VRF	VPN Routing and Forwarding	VRF is a technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses are used without conflicting with each other.

1.3 TARGET OF EVALUATION (TOE) REFERENCE

Service Router Operating System (SR OS) v7.0. The corresponding build number is 7.0.R8.

The SR OS runs on the following platforms:

a. Alcatel-Lucent 7710 Service Router (SR);
b. Alcatel-Lucent 7750 Service Router (SR); and
c. Alcatel-Lucent 7450 Ethernet Service Switch (ESS).

1.4 TOE OVERVIEW

1.4.1 Usage of the TOE

The Service Router Operating System (SR OS) is designed to provide the functionality for infrastructure class telecom equipment such as Alcatel-Lucent 7710, 7750 Service Routers (SRs) and 7450 Ethernet Service Switch (ESS). Internet Protocol (IP) and Multi-Protocol Label Switching (MPLS) networks based on the Alcatel-Lucent 7710, 7750 (collectively termed 77x0) SR and networks based on the 7450 ESS are deployed in both the service provider and enterprise environment to provide Layer 2 and Layer 3 service.

The 7710/7750 SR and 7450 ESS offer security features to address the security requirements in both network infrastructure and service layer. Service delivery access methods include: Asynchronous Transfer Mode (ATM), Synchronous Digital Hierarchy (SDH), Ethernet, and Synchronous Optical Networking (SONET). Forwarding Technology employed in the product includes Layer 2/Layer 3 encapsulation and Internet Protocol (IP), MPLS/ Media Access Control (MAC) forwarding lookup.

The 7710/7750 SR offers service providers and enterprises differentiated services, from Internet access to multipoint Virtual Private Network (VPN)[1] over a single network infrastructure. The 7450 ESS enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/ MPLS-based networks.

The major security features of the SR OS are audit, Identification & Authentication (I&A), security management, access to the product, and information flow control (i.e., network packets sent through the TOE are subject to router information flow control rules setup by the administrator). The SR OS also provides protection against the Denial of Service (DoS) attacks.

1.4.2 TOE Type

The TOE is a Service Router (SR) / Ethernet Service Switch (ESS).

Alcatel-Lucent 7710, 7750 Service Routers (SRs) are deployed in a multi-service edge routing environment, while the 7450 Ethernet Service Switches (ESSs) are deployed in a Metro Ethernet/MPLS aggregation environment.

[1] VPN is a capability of the SR OS; however, it is defined outside the TOE and not evaluated.

1.4.3 Non-TOE Hardware

The TOE is a software (and Control Processor Module (CPM) hardware) TOE consisting of the Alcatel-Lucent Service Router Operating System (SR OS) which is an integral component of the Alcatel-Lucent service router product family, which includes the:

a. Alcatel-Lucent 7710 Service Router (SR) (models SR-c4, SR-c12);
b. Alcatel-Lucent 7750 Service Router (SR) (models SR-1, SR-7 and SR-12); and
c. Alcatel-Lucent 7450 Ethernet Service Switch (ESS) (models ESS-1, ESS-6, ESS-7 and ESS-12.i

The hardware for the above listed models is excluded from the TOE boundary with the exception of CPM hardware queues for the 7710 SR-c4 and SR-c12, 7750 SR-7 and SR-12, and ESS-6, ESS-7 and ESS-12i models which are included in the TOE boundary. Administrators allocate dedicated CPM hardware queues for certain traffic designated to the CPUs and set the corresponding rate-limit for the queues.[2]

For the various models there are only performance (number of I/O modules, thru-put, redundancy, capacity) differences and no security related differences. Security features, their behaviors, and the way they configured are the same both in 7710/7750 SR and 7450 ESS.

There is also the 5620 Service Aware Manager (SAM) which provides GUI management functions (e.g., provisioning) for the 7710, 7750 & 7450. The 5620 is defined outside the TOE boundary with a Console Command Line Interface (CLI) (provides administrators with backside services) also outside the TOE boundary. Both the 7710/7750 SR and the 7450 ESS can be managed by the 5620 SAM. The 5620 SAM includes the Element Manager (SAM-E), Provisioning (SAM-P), and Assurance (SAM-A) modules. In the deployed configuration of the TOE in its intended environment, the primary means of administering the TOE during normal operations will be via local/remote Console/CLI access.

The operational environment requires a RADIUS or TACACS+ server for authentication/ authorization services, the SAM for remote administration, local Console access, SNMP/Syslog servers for logging, and a Network Time Protocol (NTP) server for external time synchronization.

Minimum hardware and operating system requirements for the external IT entities connected to the TOE are:

a. RADIUS/TACACS+ server: Any combined hardware and operating system platform that supports RFC 2865 (Authentication & Authorization) and RFC 2866 (Accounting) for RADIUS. Any combined hardware and operating system platform that supports RFC 1492 for TACACS+;

[2] A CPM filter is a hardware filter that applies to all the traffic going to the CPM CPU. It is used to drop, accept packets, as well as allocate dedicated hardware queues for the traffic.

b. SAM: SUN Solaris 10 or any 32-bit Windows operating system;
c. SCP/remote CLI: Any combined hardware and operating system platform that supports the operation of the Secure Shell protocol;
d. SNMP/Syslog server: Any combined hardware and operating system platform that supports RFC 3411-RFC 3418 for Simple Network Management Protocol version 3. Any combined hardware and operating system platform that supports RFC 5424 The Syslog Protocol;
e. Local Console/CLI: Any combined hardware and operating system platform that supports terminal emulation to the ANSI X3.64 standard;
f. NTP server: Any combined hardware and operating system platform that supports RFC 1305 for Network Time Protocol.

1.4.4 TOE Operational Environment

General

The SR/ESS has the ability to monitor, route, and manipulate network traffic to facilitate its delivery to the proper destination on a network or between networks. The SR/ESS is placed at the edge of a given network or network segment. In the case of residential aggregation, there are broadband service access nodes and aggregator devices between the SR/ESS and the actual customer. There is typically a residential gateway in between the SR/ESS and the actual customer, which is a managed device from the service provider. For business services there is either another level of aggregation switches and Customer Premise Equipment (CPE) between the SR/ESS and the customer network.

For the SR/ESS to function it must have at least two distinct networks or network segments to pass data between. The SR/ESS is a device that forwards data packets along networks. The SR/ESS is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.

Between SR/ESSs, network control information is exchanged via channels to allow dynamic connection establishment and packet routing. Network control information consists of specific requests and instructions that include destination address, routing controls, and signalling information.

Physical Installation, Deployed Configuration and Interfaces

All TOE interfaces shown in Figure 1, with the exception of the network traffic/data interface are attached to the internal (trusted) network. The network traffic/data interface is attached to internal and external networks. The Console Access via RS-232 interface is a direct local connection.

The physical boundary is the SR OS located on a compact flash card. The SR OS runs on various hardware platforms.

The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

Fully authorized administrators with access to data have low motivation to attempt to compromise the data because of other assumptions and organization security policies defined herein.

The deployment configuration of the TOE in its intended environment is to be at least as restrictive as the baseline evaluated configuration defined herein and is to be configured in accordance with operational user/preparative guidance documentation. All administrators are assumed to be "vetted" to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

Using the concept of separation of duties each administrator can have a defined function in respect to the operations aspect of the SR/ESS. Each administrator can only be provided enough access to perform their duties on the network and no more.

The deployed configuration of the TOE provides automatic detection of attacks triggered by excessive control plane and routing protocol traffic, and it recognizes signatures of some common Distributed and other DoS (D/DoS) attacks and further it will suppress these attacks using filters and Access Control Lists (ACLs.

The operational environment is responsible for providing the TOE with the necessary trusted path/channel interfaces. Remote management traffic (to/from the TOE) will be protected using SSH[3] or SCP (secure copy) and remote telnet will be disabled.

SR OS Services Guide - Alcatel-Lucent Service Model

Services are provisioned on the SR/ESSs and transported across an IP and/or IP/MPLS provider core network in encapsulation tunnels created using generic router encapsulation (GRE) or MPLS label switched paths (LSPs).

Best practices are recommended regarding:

a. CPM filter (default action deny) and using exhaustive list of all inband protocols authorized and explicitly denied; and
b. Management access filters (restrict IP addresses that should have remote access (list allowed addresses and deny others).

The Management Ethernet port on the TOE has a completely independent routing instance named "management" distinct from all in-band routing instances. Any out-of-band traffic received on the Management Ethernet port cannot be forwarded out of any in-band ports and vice versa.

The service model uses logical service entities to construct a service. The logical service entities are designed to provide a uniform, service-centric configuration, management, and billing model for service provisioning.

[3] SSH/SCP communications is a capability of the SR OS; however, the underlining crypto protocols are defined outside the TOE and part of the TOE's operation environment and not evaluated. TSFI(2) (see Figure 1) is evaluated.

Service provisioning uses logical entities to provision a service where additional properties are configured for bandwidth provisioning, QoS, security filtering to the appropriate entity.

Each subscriber service type is configured with at least one service access point (SAP). A SAP identifies the customer interface point for a service on an Alcatel-Lucent SR/ESS-Series router. The SAP configuration requires that slot, MDA, and port/channel information be specified. The slot, MDA, and port/channel parameters must be configured prior to provisioning a service.

A service distribution point (SDP) acts as a logical way to direct traffic from one router to another through a uni-directional (one-way) service tunnel. The SDP terminates at the far-end device which directs packets to the correct service egress SAPs on that device. A distributed service consists of a configuration with at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service to the service tunnel.

Delivery of services requires a number of operations occur properly and at different levels in the service delivery model. In order to verify that a service is operational, a set of in-band, packet-based Operation, Administration, and Maintenance (OAM) tools is used, with the ability to test each of the individual packet operations.

1.5 TOE DESCRIPTION

1.5.1 General

The three TOE/product subsystems that directly implement the SR OS security features for infrastructure/ service layer are:

a. Management Plane subsystem;
b. Control Plane subsystem; and
c. Data Plane subsystem.

The SR-Series software uses a base real-time operating system (OS). The primary copy of SR OS software is located on a compact flash card in the hardware platforms. The removable media is shipped with each router and contains a copy of the SR OS image.

1.5.2 Management Plane subsystem

In the infrastructure layer, the security features for management plane address security needs associated with network management activities for the SR network elements.

The Management plane provides configuration control and the connection of statistics and state information for reporting. Security capabilities are implemented in this plane. It provides other planes configuration information and receives statistics and state information from other planes.

Management Access Filter
The Management Access Filter (MAF) restricts access to the SR to small list of servers or support workstations. MAFs are used to restrict traffic on Out-of-band (OOB) Ethernet ports. The MAFs are enforced in software and control all traffic going into the Control Processor Module (CPM), including all routing protocols. MAFs apply to packets from all ports and they are used to restrict management of the SR/ESS router by other nodes outside either specific (sub) networks or through designated ports.

MAFs allow the operator to configure the following: Destination UDP/TCP port number, IP protocol ID, Source port, and Source IP address. The MAF entries are explicitly created on each router. When the first match is found actions are executed. Entries are sequenced from most to least explicit.

Login Control parameters (for Console, Remote management[4]). Parameters include exponential-back off, idle-time, inbound-max-sessions and login-banner. Exponential-back off parameter enables the exponential-back off of the login prompt to deter dictionary attacks. Idle-time parameter configures the sessions idle timeout to prevent unauthorized access through an unattended opened session.

Profiles. Administrator profiles are configured to permit or deny access to a hierarchical branch or specific commands. Depending on the authorization requirements, passwords are configured locally or on a RADIUS server. Profiles also specify which protocols are allowed by the administrator to access the system.

Authentication, Authorization. Access permission to the system are controlled using: TACACS+; RADIUS; or, local to the element. A profile, which is based on administrator name and password configurations, is applied for the administrator authorization processes. RADIUS, and TACACS+ are supported on all TOE interfaces including the console port. This ST addresses TOE (client-side) support of RADIUS and TACACS+ where external authentication services are available via either RADIUS, TACACS+, or both.

1.5.3 Control Plane subsystem

The Control plane handles the dynamic protocols for the exchange of forwarding information. It provides other planes with protocols and services information and receives configuration and state information from others.

The Control Plane consists of all software modules that interact with or control how traffic is forwarded through an individual node or the entire network. This includes routing and services protocols as well as OAM functionality.

[4] SSH secure communications is a capability of the SR OS; however, the underlining crypto protocols and associated cryptographic functionality are defined outside the TOE and part of the TOE's operational environment and not evaluated.

CPM filters control all traffic going in to the CPM, including all routing protocols. They apply to packets from all network and access ports, but not to packets from a management Ethernet port. CPM packet filtering and queuing is performed by network processor hardware using no resources on the main CPUs.

The control plane functions are mainly located in the CPM of a SR/ESS. The Switch Fabric (SF)/ Control Processor Module (CPM) controls the switching and routing and functions of the TOE.

The SR/ESS provides CPM protection against the DoS attacks.

Filters can be installed for ingress management traffic destined either for the CPM Ethernet port or any other logical port (LAG, port, or channel) on the device to be subject of the filter-action.

MAC/IP CPM filters and queues control all traffic going into the CPM, including all routing protocols. They apply to packets from all network and access ports, but not to packets from a management Ethernet port. MAC CPM filters or IP CPM filters are used to perform a match and apply action using filter criteria.

Packets going to the CPM are first classified by the Input Output Module (IOM) into forwarding classes (FCs) before CPM hardware sees them. CPM filters are used to further classify the packets using Layer 3/Layer 4 information. CPM filters are applied before IP reassembly. All encapsulation types are supported, e.g., Ethernet, FR, PPP, etc. For the CPM filter the default action is “DENY” with an exhaustive list of all in-band protocols authorized and explicitly denied.

The Route Table Manager (RTM) is a library with its own dedicated memory manager. RTM modification APIs are invoked from Routing Protocols. Routing protocols implemented are: OSPFv2, IS-IS, BGP-4, MPLS (LDP, RSVP-TE).

1.5.4 Data Plane subsystem

The Data plane handles the forwarding of customer data. It provides other planes with statistics and state information and receives configuration information for services and forwarding information for the handling of data.

Using the Quality of Service (QoS) and Access Control List (ACL) capabilities of the SR-OS DoS activity can be mitigated. These acts can be thought of in terms either “to” the routers or “through” the routers. ACL’s are used to protect against the “to” DoS and CPM queues used for the “through”.

The Data Plane subsystem applies Access control lists (ACLs) filter policies on ingress or egress to an interface or service. The Data Plane subsystem provides two types of traffic filters: ip-filters and mac-filters. Addresses can be restricted to known MAC/IP’s; an ACL can be created and maintained to restrict access to the device based on MAC/IP’s.

An ACL or Filter Policy is a filter template. Filter Policies can be applied on ingress or egress to a service access point on an interface thus allowing the specification of customer specific access control. The ACL can be used to prevent the un-known party (identified by IP match or MAC match criteria) to access the switch's infrastructure and service layer, and provide security protections of both layers.

Typically traffic associated with a customer service or standard routing flow is completely handled by the data plane and cannot reach the control or network management planes. In some cases certain data entering via the data plane may be redirected to the control plane for exception processing such as: protocol related packets, OAM packets and error packets.

1.5.5 Out-Of-Band Management Interfaces

Out-of-band interfaces use terminal emulation software and connect to the RS-232 Console port on the TOE or through a remote session using the management Ethernet port on the TOE.

Any out-of-band traffic received on the Management Ethernet port cannot be forwarded out of any in-band ports and vice versa.

1.5.6 In-Band Management Interface

In-band Management Interface involves management sessions to one of the SR OS IP interfaces using a physical I/O port on the device.

1.5.7 Secure Copy Protocol (SCP)

The administrator copies and manages software images, configuration files and log files via SCP[5]. All of these functions are performed through in-band interfaces and the OOB management Ethernet port.

1.5.8 Local Console Access

Local authentication[6] uses administrator names and passwords to authenticate login attempts.

[5] Secure Copy Protocol (SCP) is a capability of the SR OS; however, the underlining crypto protocol and associated cryptographic functionality is defined outside the TOE and part of the TOE's operational environment and is not evaluated.

[6] To establish a console connection, an ASCII terminal or a PC running terminal emulation software is used, set to parameters: baud rate 115,200, data bits 8, parity none, stop bits 1, flow control none.

1.5.9 Physical scope

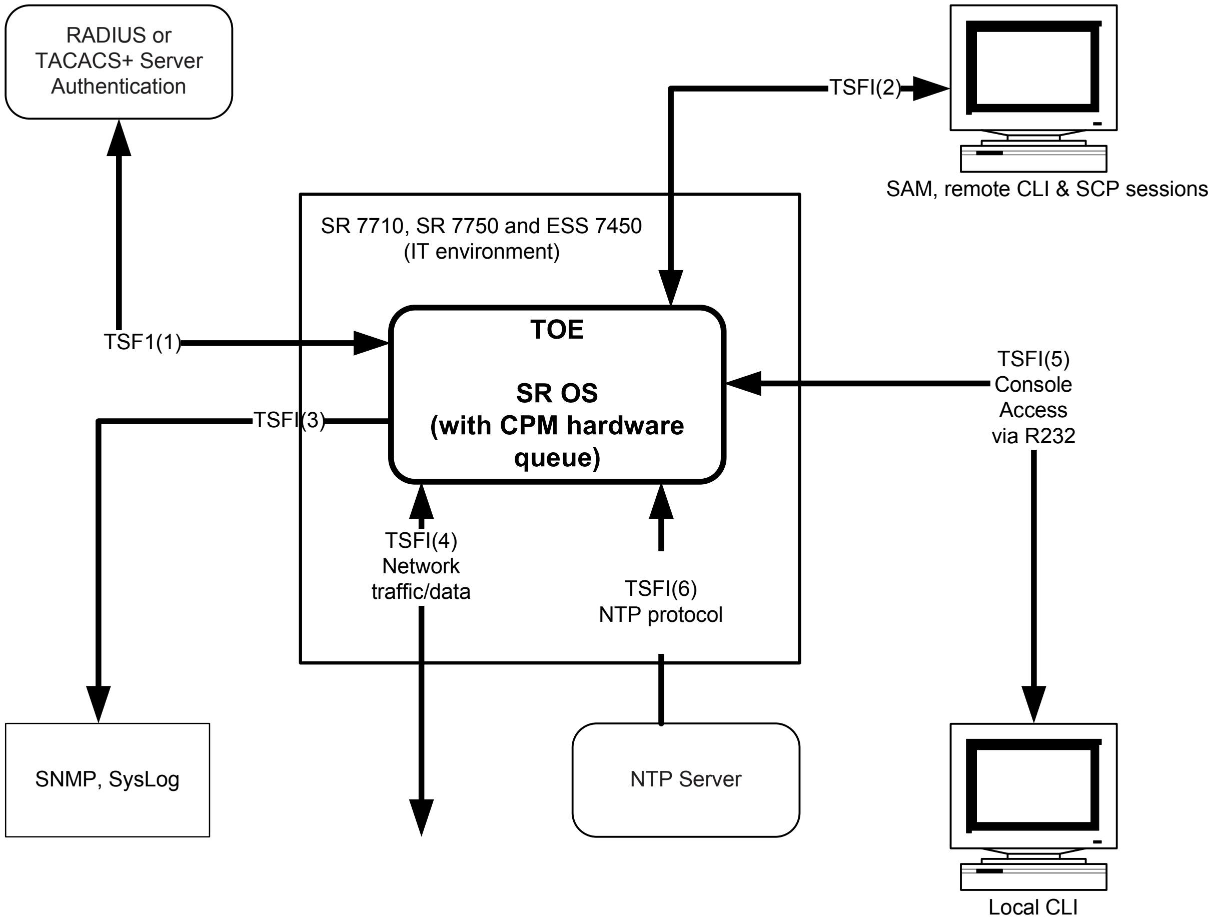

RADIUS or TACACS+ Server Authentication
TSFI(2)
SAM, remote CLI & SCP sessions
SR 7710, SR 7750 and ESS 7450 (IT environment)
TSF1(1)
TOE
SR OS (with CPM hardware queue)
TSFI(5) Console Access via R232
TSFI(3)
TSFI(4) Network traffic/data
TSFI(6) NTP protocol
SNMP, SysLog
NTP Server
Local CLI

Figure 1 - TOE Boundary

<u>Note to Figure 1</u>: The physical boundary is the SR OS v7.0 located on a compact flash card. The SR OS v7.0 runs on various hardware platforms but the hardware platforms are excluded with the exception of the CPM hardware queues. Administrators allocate dedicated CPM hardware queues for certain traffic designated to the CPUs and set the corresponding rate-limit for the queues. These CPM hardware queues are included in the TOE boundary. The TOE's operational environment requires a RADIUS or TACACS+ server for authentication/authorization services, the SAM for limited remote administration, local Console access for most administration, SNMP/Syslog servers for logging, and a Network Time Protocol (NTP) server for external time synchronization. All TSFIs are evaluated.

1.5.10 Logical Scope

The logical boundaries of the TOE are defined by the functions that are carried out by the TOE at the TOE external interfaces. The TOE addresses the following security relevant features:

1.5.10.1 Audit

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system.

Audit also keeps track of the activity of an administrator who has accessed the network. The type of audit information recorded includes a history of the commands executed, the amount of time spent in the session, the services accessed, and the data transfer size during the session.

1.5.10.2 Identification/Authentication & Authorization (I/A& A)

Network security for the SR OS is based on a multi-step process. The first step, identification/ authentication, validates a administrator's name and password. The second step is authorization, which allows the administrator to access and execute commands at various command levels based on profiles assigned to the administrator.

1.5.10.3 Security Management

The Administrator configures system security and access functions and logging features using CLI syntax and command usage to configure parameters.

1.5.10.4 TOE Access

Mechanisms place controls on administrator's sessions. Local and remote administrator's sessions are dropped after an Administrator-defined time period of inactivity. Dropping the connection of a local and remote session (after the specified time period) reduces the risk of someone accessing the local and remote machines where the session was established, thus gaining unauthorized access to the session.

1.5.10.5 User data protection (Information flow control)

The SR OS enforces an UNAUTHENTICATED SFP whereby the network packets sent through the TOE are subject to router [information flow control] rules setup by the administrator.

The SR OS enforces an AUTHENTICATED SFP whereby information is passed via application proxy (Console, SAM, SNMP). Users must first be granted access by the administrator and then authenticated in order to access the router by Console, SAM, or SNMP.

The SR OS enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap and Syslog destinations.

1.5.10.6 TSF Protection (Availability)

The SR OS ensures the availability of security parameters exchanged from the TOE to/ from RADIUS/TACACS+ servers (in the operational environment).

The SR OS also ensures the availability of security parameters imported from NTP servers (in the operational environment) to the TOE.

1.5.10.7 Local/remote Console Access

Local/remote console authentication access to the router uses administrator names and passwords to authenticate login attempts.

1.5.11 Evaluated Configuration

The evaluated configuration for the TOE must include the following enabled/disabled/configured (all other services, protocols and settings are excluded from the evaluated configuration):

a. Enable SR OS (CLIENT-side) for RADIUS or TACACS+ server authentication/ authorization services, the SAM for limited remote administration, local Console access for most administration, SNMP/Syslog servers for logging, and a Network Time Protocol (NTP) server for external time synchronization.
b. Enable Routing protocols from this set: OSPFv2, IS-IS, BGP-4, MPLS (LDP, RSVP-TE).
c. Ensure Telnet remains disabled.
d. Use SNMPv3 only.
e. Configure MAF filters to restrict access to management ports on the appliance.
f. Configure CPM Filters for DoS attack protection against router appliance and network.
g. Configure CPM Queues for bandwidth restrictions as a protection again DoS attacks targeting the network.
h. Configure Anti-spoofing.
i. Configure QoS to mitigate DoS and worm type of behaviour.
j. Configure Border Gate Protocol (BGP) and Label Distribution Protocol (LDP) Time to Live (TTL) Security.
k. Enforce/enable/configure a strong password policy.
l. Disable sending events to a console destination. The console device is not be used as an event log destination. A log created with the console type destination displays events to the physical console device. Events are displayed to the console screen whether an administrator is logged into the console or not.

1.5.12 TOE Guidance Documents

The guidance documents that accompany the TOE are:

a. 7450 ESS OS Basic System Configuration Guide
b. 7450 ESS OS System Management Guide
c. 7450 ESS OS Interface Configuration Guide
d. 7450 ESS OS Router Configuration Guide
e. 7450 ESS OS Routing Protocols Guide
f. 7450 ESS OS MPLS Guide
g. 7450 ESS OS Services Guide
h. 7450 ESS OS OAM and Diagnostic Guide
i. 7450 ESS OS Triple Play Guide
j. 7450 ESS Quality of Service Guide
k. 7450 ESS-Series OS Integrated Services Adapter Guide

l. 7710 SR OS Basic System Configuration Guide
m. 7710 SR OS System Management Guide
n. 7710 SR OS Interface Configuration Guide
o. 7710 SR OS Router Configuration Guide
p. 7710 SR OS Routing Protocols Guide
q. 7710 SR OS MPLS Guide
r. 7710 SR OS Services Guide
s. 7710 SR OS OAM and Diagnostic Guide
t. 7710 SR OS Triple Play Guide
u. 7710 SR Quality of Service Guide

v. 7750 SR OS Basic System Configuration Guide
w. 7750 SR OS System Management Guide
x. 7750 SR OS Interface Configuration Guide
y. 7750 SR OS Router Configuration Guide
z. 7750 SR OS Routing Protocols Guide
aa. 7750 SR OS MPLS Guide
bb. 7750 SR OS Services Guide
cc. 7750 SR OS OAM and Diagnostic Guide
dd. 7750 SR OS Triple Play Guide
ee. 7750 SR Quality of Service Guide
ff. 7750 SR-Series OS Integrated Services Adapter Guide

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA (CC) CONFORMANCE

This ST has been prepared in accordance with and is conformant to:

a. Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, Revision 2, September 2007 (CCMB-2006-09-001, CCMB-2007-09-002, CCMB-2007-09-003)

b. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007 (CCMB-2007-09-004).

The ST is CC Parts 2 and 3 conformant and contains an extended security requirement (EXT_FPT_ITA Availability of Imported TSF Data).

2.2 PROTECTION PROFILE (PP) CONFORMANCE

None.

2.3 EVALUATION ASSURANCE LEVEL (EAL)

EAL2 + (augmented with ALC_FLR.1 (Basic flaw remediation))

3 SECURITY PROBLEM DEFINITION

The security problem definition shows the threats, Organizational security policies (OSPs) and assumptions that must be countered, enforced and upheld by the TOE and its operational environment.

3.1 THREATS

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

The threats listed below are addressed by the TOE. The threat agents consist of unauthorized persons or external IT entities that are not authorized to use the TOE as well as authorized administrators of the TOE who make errors in configuring the TOE.

The threat agents are divided into two categories:

a. Attackers who are not TOE administrators: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.

b. TOE administrators: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE administrators are, however, assumed not to be wilfully hostile to the TOE.)

The assumed level of expertise of the attacker for all the threats is unsophisticated. Both threat agents are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network.

Considering the possible attack scenarios for the deployed configuration of the TOE in its intended environment, the level of attack potential assumed for the attacker is BASIC which is in keeping with the desired EAL2+ assurance level of this TOE, considering factors of attackers' expertise, resources, opportunity and motivation.

Fully authorized administrators with access to data have low motivation to attempt to compromise the data because of other assumptions and organization security policies defined herein.

T.AUDIT Actions performed by administrators (modification of TOE and network infrastructure and service layer system security configuration/parameters) may not be known to the administrators due to actions not being recorded (and time stamped) or the audit records not being reviewed prior to the machine shutting down, or an unauthorized administrator modifies or destroys audit data.

T.TSF_DATA A malicious administrator may gain unauthorised access to inappropriately view, tamper, modify, or delete TOE Security Functionality (TSF) data.

T.MEDIATE An unauthorized entity may send impermissible information through the TOE which results in the exploitation (e.g., destruction, modification, or removal of information and/or other resources), and/or exhaustion of resources on the network (e.g. bandwidth consumption or packet manipulation).

T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session and view and change the TOE security configuration.

T.UNAUTH_MGT_ACCESS An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.

3.2 ASSUMPTIONS

This section of the security problem definition shows the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions are on physical, personnel and operational environment.

3.2.1 Personnel Assumptions

A. ADMINISTRATOR

The authorized administrators are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance, and will periodically check the audit record; however, they are capable of error. Personnel will be trained in the appropriate use of the TOE to ensure security.

3.2.2 Physical Environment Assumptions

A.CONNECTIVITY

All TOE external interfaces except for the network traffic/data interface are attached to the internal (trusted) network. This includes: (1) the RADIUS, TACACS+ server interface; (2) the SAM, SCP interface; (3) the SNMP, Syslog interface; and (4) the NTP interface. The Network traffic/data interface is attached to internal and external networks. Console Access is via RS-232, a direct local connection in the same physical location as the TOE.

A.LOCATION

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

A.PHYSICAL

It is assumed that the operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

3.2.3 Operational Assumptions

A.GENPURPOSE There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.EXT_AUTHORIZATION External authentication services will be available via either RADIUS, TACACS+, or both, based on defined Internet Engineering Task Force (IETF) standards.

A.INTEROPERABILITY The TOE functions with the external IT entities shown in Figure 1 herein and with other vendors' routers on the network and meets Request for Comments (RFC) requirements for implemented protocols.

A.TIMESTAMP The operational environment provides the TOE with the necessary reliable time stamp. External Network Time Protocol (NTP) services will also be available to provide external time synchronization.

A.TRUSTED_PATH/CHANNEL[7] The operational environment provides the TOE with the necessary trusted path/channel interfaces. Remote management traffic (to/from the TOE) will be protected using SSH or SCP (secure copy) and remote telnet will be disabled.

The Operational Environment will protect remote administrative sessions from eavesdropping. The Operational environment will provide a means to ensure that administrators are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.

The operational environment will protect communications with remote external IT entities. The operational environment will ensure that the communication channel is logically distinct from other communication channels.

The Operational environment will assure identification of its end points and protection of the channel data from modification or disclosure.

The Operational environment will permit itself to initiate communication via the trusted channel.

[7] SSH/SCP communications is a capability of the SR OS; however, the underlining crypto protocols are defined outside the TOE and part of the TOE's operation environment and not evaluated. TSFI(2) (see Figure 1) is evaluated.

3.3 ORGANIZATIONAL SECURITY POLICIES

Application Note: Organizational security policies may be defined by the end-user of the TOE. The TOE developer provides procedural security recommendations to the purchaser of the TOE.

P.CONSOLE	In the deployed configuration of the TOE in its intended environment, the primary means of administering the TOE during normal operations will be via local/remote Console/CLI access.
P.DEPLOYED_CONFIG	The deployed configuration of the TOE in its intended environment shall be at least as restrictive as the baseline evaluated configuration defined herein and will be configured in accordance with guidance documentation.
P.USERS	The TOE is administered by one or more Administrators who have been granted rights to administer the TOE. All administrators are "vetted" to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

4 SECURITY OBJECTIVES

The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition.

4.1 SECURITY OBJECTIVES FOR THE TOE

The following are the IT security objectives for the TOE:

O.AUDIT

The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event. The TOE will provide the privileged administrators the capability to review Audit data and will restrict audit review to administrators who have been granted explicit read-access.

O.MANAGE

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

O.I&A

The TOE will uniquely identify and authenticate the claimed identity of all administrative administrators before granting management access and to control their actions.

O.MEDIATE

The TOE must mediate the flow of all information between hosts located on disparate internal and external networks governed by the TOE. The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.

O.TOE_ACCESS

The TOE will provide mechanisms that control a administrator's logical access to the TOE and to explicitly deny access to specific administrators when appropriate.

For a detailed mapping between threats and the IT security objectives listed above see Section 8.1 of the Rationale.

4.2 IT SECURITY OBJECTIVES FOR THE ENVIRONMENT

The following IT security objectives for the environment[8] are to be addressed by the Operational environment via technical means.

OE.TIME	The operational environment will supply the TOE with a reliable time source.
OE.EXT_AUTHORIZATION	A RADIUS server, a TACACS+ server, or both must be available for external authentication services.
OE.TRUSTED PATH/ CHANNEL	The Operational environment will provide the TOE with the necessary trusted path/channel interfaces. The Operational environment for the SR OS will support Secure Shell Version 2 (SSH) a protocol that provides a secure, connection to the router. A connection is always initiated by the client (the administrator). Authentication takes places by one of the configured authentication methods (local, RADIUS, or TACACS+). SSH allows for a secure connection over an insecure network.
OE.GENPURPOSE	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities for the TOE in its operational environment.
OE.INTEROPERABILITY	The external IT entities shown in Figure 1 herein will be able to function with the TOE and with other vendors' routers on the network and meet Request for Comments (RFC) requirements for implemented protocols.
OE.CONNECTIVITY	All TOE external interfaces except for the network traffic/data interface are attached to the internal (trusted) network. This includes: (1) the RADIUS, TACACS+ server interface; (2) the SAM, SCP interface; (3) the SNMP, Syslog interface; and (4) the NTP interface. The Network traffic/data interface is attached to internal and external networks. Console Access is via RS-232, a direct local connection in the same physical location as the TOE.

[8] Secure Copy Protocol (SCP) and SSH secure communications are capabilities of the SR OS; however, the underlining crypto protocols and associated cryptographic functionality are defined outside the TOE and part of the TOE's operational environment and not evaluated. TSFI(2) (see Figure 1) is evaluated. This ST addresses TOE (client-side) support of RADIUS and TACACS+ where external authentication services are available via either RADIUS, TACACS+, or both. RADIUS or TACACS+ authentication servers or NTP servers with which the SR OS communicates are considered external IT entities that are part of the TOE's operational environment. The operational environment for the SR OS requires a RADIUS or TACACS+ server and the SAM for remote administration and a Network Time Protocol (NTP) server for external time synchronization.

OE.DEPLOYED_CONFIG The deployed configuration of the TOE in its intended environment shall be at least as restrictive as the baseline evaluated configuration defined herein and will be configured in accordance with a guidance documentation

OE.CONSOLE In the deployed configuration of the TOE in its intended environment, the primary means of administering the TOE during normal operations will be via local/remote Console/CLI access.

4.3 NON-IT SECURITY OBJECTIVES FOR THE ENVIRONMENT

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures:

OE.ADMINISTRATOR The authorized administrators are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance (e.g., procedures to review/manage audit records); however, they are capable of error. Personnel will be trained in the appropriate use of the TOE to ensure security.

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

OE.PHYSICAL The operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

OE.USERS All administrators are “vetted” to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

5 EXTENDED COMPONENTS DEFINITION

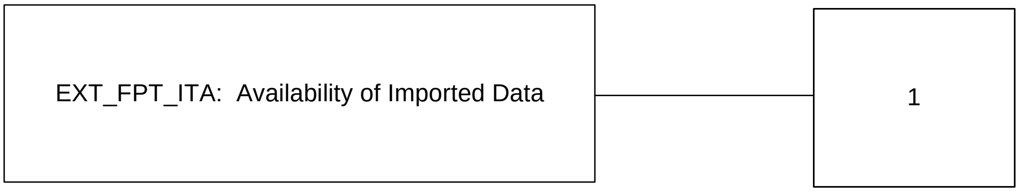
This section specifies the extended SFRs for the TOE.

5.1 EXT_FPT_ITA AVAILABILITY OF IMPORTED TSF DATA

Family Behaviour

This family defines the rules for the prevention of loss of availability of TSF data moving between another trusted IT product and the TSF. This data could, for example, be TSF critical data such as passwords, keys, audit data, or TSF executable code. This extended requirement was created because the CC Part 2 does not include a SFR for the availability of imported data; there is only a SFR for the availability of exported data.

Component levelling



This family consists of only one component, EXT_FPT_ITA.1 Inter-TSF availability within a defined availability metric. This component requires that the TSF ensure, to an identified degree of probability, the availability of TSF data received from another trusted IT product.

Management: FPT_ITA.1

The following actions could be considered for the management functions in FMT:

a. management of the list of types of TSF data that must be available to another trusted IT product.

Audit: FPT_ITA.1

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

a) Minimal: the absence of TSF data when required by a TOE.

EXT_FPT_ITA.1 Inter-TSF availability within a defined availability metric

Hierarchical to: No other components. Dependencies: No dependencies.

EXT_FPT_ITA.1.1 The TSF shall ensure the availability of [assignment: list of types of TSF data] received from another trusted IT product within [assignment: a defined availability metric] given the following conditions [assignment: conditions to ensure availability].

6 IT SECURITY REQUIREMENTS

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance requirements from Part 3 of the CC.

The security requirements consist of two groups of requirements:

a. the security functional requirements (SFRs): a translation of the security objectives for the TOE into a standardised language; and
b. the security assurance requirements (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

6.1.1 Overview

6.1.1.1 Content

The security functional requirements for this ST consist of the following components from Part 2 of the CC, an extended component (EXT_FPT_ITA.1 Inter-TSF availability within a defined availability metric), as summarized in Table 1.

CC Part 2 Security Functional Components	
Identifier	**Name**
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FDP_ETC.2	Export of user data with security attributes
FDP_IFC.1(1)	Subset information flow control (unauthenticated policy)
FDP_IFC.1(2)	Subset information flow control (authenticated policy)
FDP_IFC.1(3)	Subset information flow control (export policy)
FDP_IFF.1(1)	Simple security attributes (unauthenticated policy)
FDP_IFF.1(2)	Simple security attributes (authenticated policy)
FDP_IFF.1(3)	Simple security attributes (export policy)
FIA_AFL.1(1)	Authentication failure handling (console)
FIA_AFL.1(2)	Authentication failure handling (exponential backoff)
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_UAU.5	Multiple authentication mechanisms
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITA.1	Inter-TSF availability within a defined availability metric
EXT_FPT_ITA.1(1)	Inter-TSF availability within a defined availability metric (RADIUS/TACACS+)
EXT_FPT_ITA.1(2)	Inter-TSF availability within a defined availability metric (NTP)
FTA_SSL.3	TSF-initiated termination

CC Part 2 Security Functional Components	
Identifier	**Name**
FTA_SSL.4	User-initiated termination
FTA_TSE.1	TOE session establishment (Remote)

Table 1 – TOE Security Functional Requirements

6.1.2 Security Functional Requirements

6.1.2.1 FAU_GEN.1 Audit data generation

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

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

b. All auditable events for the [not specified] level of audit;

c. [Log activity of administrators;

d. Log critical network traffic;

e. Logging of configuration changes; and

f. Security breach logging.

Application note *Log critical network traffic. Applications within the SR OS for which log entries are generated are: IP, routing protocols and services, and CLI and remote access.*

Logging of configuration changes. The change activity event source is all events that directly affect the configuration or operation of the TOE as defined in 6.1.2.21FMT_SMF.1 Specification of management functions and 7.1.4.4.

Security breach logging. The security event source is all events that affect attempts to breach system security such as failed login attempts, attempts to access Management Information Base (MIB) tables to which the administrator is not granted access or attempts to enter a branch of the CLI to which access has not been granted. Security events are generated by the security application.

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, and the outcome ~~(success or failure)~~ (short text description) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the ST, [none].

6.1.2.2 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.

6.1.2.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [authorized administrators] with the capability to read [all audit data] from the audit records.

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

Application Note – Above listed SFR 6.1.2.3 (FAU_SAR.1 Audit review) does not apply to the syslog and session audit files.

6.1.2.4 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.

Application Note – Above listed SFR 6.1.2.4 (FAU_SAR.2 Restricted audit review) does not apply to the syslog and session audit files.

6.1.2.5 FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the [EXPORT SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [none].

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

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

a. [subjects: each IT entity that sends and receives information through the TOE to one another;
b. information: network packets sent through the TOE from one subject to another; and
c. operations: route packets].

6.1.2.7 FDP_IFC.1(2) Subset information flow control (authenticated policy)

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

a. [source subject representing authenticated user: source network identifier;
b. destination subject: TOE interface to which information is destined;
c. information: network packets; and
d. operations: pass information via application proxy (Console, SAM, file-copy).

6.1.2.8 FDP_IFC.1(3) Subset information flow control (export policy)

FDP_IFC.1.1(3) The TSF shall enforce the [EXPORT SFP] on:

a. [subjects: each IT entity that receives information from the TOE;
b. information: events sent from the TOE to SNMP trap, Syslog and RADIUS/TACACS+ destinations; and
c. operations: send events].

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

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

a. [security subject attributes:

i) IP network address and port of source subject;

ii) IP network address and port of destination subject;

iii) transport layer protocol and their flags and attributes (UDP, TCP);

iv) network layer protocol (IP, ICMP);

v) Documented Special Use (DUSA) IPv4 addresses;

vi) interface on which traffic arrives and departs; and

vii) routing protocols and their configuration and state].

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:

a. the identity of the source subject is in the set of source subject identifiers (i.e., addresses);

b. the identity of the destination entity is in the set of destination entity identifiers (i.e., addresses);

Application Note: The set of identifiers are associated with the physical router interfaces.

c. the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by the Administrator) according to the following algorithm [First match. When multiple policy names are specified, the policies shall be executed in the order they are specified. The first policy that matches is applied;

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

FDP_IFF.1.3(1) The TSF shall enforce:

a. Each IFF filter policy must consist of at least one filter entry. Each entry shall consist of a collection of filter match criteria. When packets enter the ingress or egress ports, packets shall be compared to the criteria specified within the entry or entries.

b. For packet matching criteria as few or as many match parameters are specified as required, but all conditions must be met in order for the packet to be considered a match and the specified action performed. The process stops when the first complete match is found and then executes the action defined in the policy entry, either to drop or forward packets that match the criteria.

c. automatic detection of attacks triggered by excessive control plane and routing protocol traffic, and recognize signatures of some common Distributed and other DoS (D/DoS) attacks and further suppress these attacks using filters and Access Control Lists (ACLs).

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

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

a. [the TOE shall reject requests for access or services where the source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

Application Note: The intent of this requirement is to ensure that a user cannot send packets originating on one TOE interface claiming to originate on another TOE interface.

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

Application Note: A broadcast identity is one that specifies more than one host address on a network. It is understood that the TOE only knows the sub-netting configuration of networks directly connected to the TOE's interfaces and therefore is only aware of broadcast addresses on those networks.

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

d. The TSF shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table.

e. The TSF shall deny information flows that do not conform to their associated published protocol specification (e.g., RFCs for supported router protocols).

f. The TSF shall deny information flows based on filter policies (access control lists (ACLs)) selectively blocking traffic matching criteria from ingressing or egressing the TOE. Filter policies shall control the traffic allowed in or out of the TOE based on MAC or IP match criteria. Non-matching packets shall be dropped/denied.

g. When packets arrives at TOE that are not destined to any of the SR OS network management interfaces they will be either dropped or forwarded in accordance with the type of service, ACL, policies configured.

h. The TSF shall block traffic going to a destination address based on a prefix received from a customer.

6.1.2.10 FDP_IFF.1(2) Simple security attributes (authenticated policy)

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

a. [Source subject security attributes: source port and IP protocol ID and address, username/password and profile, source network identifier, remote or console session idle timeout, maximum number of concurrent inbound remote sessions, administrator permission for remote or console access, local home directory for the administrator for remote or console access;

b. Destination subject security attributes: set of destination subject identifiers *(UDP/TCP port number)*; and

c. Information security attributes: authenticated identity of source subject; identity of destination subject; transport layer protocol; and destination subject service identifier (TCP destination port number).

Application Note: "Service identifier" specifies a service that is above the network and transport layers in the protocol stack.

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

a. the source subject has successfully authenticated to the TOE;

b. the identity of the destination subject is in the set of destination identifiers;

c. the information security attributes match the attributes in a information flow policy rule (contained in the information flow policy ruleset defined by the administrator) according to the following algorithm [first match]; and

d. the selected information flow policy rule specifies that the information flow is to be permitted via the authenticated proxy selected by the rule].

FDP_IFF.1.3(2) The TSF shall enforce:

a. Any packet that is destined to the TOE, has to have the correct MAC address, and IP address assigned by the network operator to be able to remotely operate the TOE.

b. Management access filters to control all traffic in and out of the TOE and to restrict management of the TOE by other nodes outside either specific (sub) networks or through designated ports. Management access filters allow the operator to configure the following:

i) Destination UDP/TCP port number;

ii) IP protocol ID;

iii) Source port; and

iv) Source IP address.

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: [

a. Profiles shall be used to permit access to a hierarchical CLI branch or specific CLI commands. Commands matching the entry command match criteria will be permitted.

b. Profiles shall be referenced in a administrator configuration].

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

6.1.2.11 FDP_IFF.1(3) Simple security attributes (export policy)

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

[Source subject security attributes: source network identifier; and

Destination subject security attributes:

a. Syslog server IP address;

b. UDP port used to send the syslog message;

c. Syslog Facility Code;

d. Syslog Severity Threshold;

e. IP address of the SNMP trap receiver;

f. UDP port used to send the SNMP trap;

g. SNMPv3 used to format the SNMP notification;

h. Security name and level for SNMPv3 trap receivers; and

i. RADIUS/TACAS+ audit data].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a source subject and a destination subject via a controlled operation if the following rules hold:

a. [the identity of the destination subject is in the set of destination identifiers;

b. the information security attributes match the security attributes defined by the administrator) according to the following algorithm [ALL the security attributes must match]; and

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

FDP_IFF.1.3(3) The TSF shall enforce the [none].

FDP_IFF.1.4(3) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.2.12 FIA_AFL.1(1) Authentication failure handling (console)

FIA_AFL.1.1(1) The TSF shall detect when [an administrator configurable positive integer (within a range of values 1 – 64), within [an administrator configurable period of time (within a range of values 0 — 60 minutes)], unsuccessful authentication attempts occurs related to [any claimed administrator ID attempting to authenticate to the TOE].

FIA_AFL.1.2(1) When the defined number of unsuccessful authentication attempts has been met, the TSF shall [at the option of the Administrator prevent the administrators except the administrator from performing activities that require authentication until an action is taken by the Administrator, or until an Administrator defined time period (within a range of values 0 - 1440 minutes) has elapsed].

6.1.2.13 FIA_AFL.1(2) Authentication failure handling (exponential backoff - Console)

FIA_AFL.1.1(2) The TSF shall detect when [one (1)], within [an administrator configurable period of time, (within a range of values 0 – 60 minutes)], unsuccessful authentication attempts occurs related to [any claimed administrator ID attempting to authenticate to the SR OS via the local/remote Console].

FIA_AFL.1.2(2) When one (1) unsuccessful authentication attempt has been met, the TSF shall [exponentially increase the delay between subsequent login attempts].

Application Note: *Only applicable when person tries to log in to a device via console.*

6.1.2.14 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets (passwords) meet:[

a. a minimum length (characters) default 6 and within a range of 1-8,

b. the maximum length shall be up to 20 characters if unhashed, and 32 characters if hashed;

c. Complexity requirements: [numeric] [special-character] [mixed-case]

   i) at least one (1) numeric character must be present in the password; and

   ii) at least one (1) special character must be present in the password. Special characters include: ~!@#$%^&*()_+|{}:”<>?`-=\[];’

   iii) at least one (1) upper and one (1) lower case character;

d. An administrator defined number of days an administrator password is valid before the administrator must change their password. This parameter shall be used to force the administrator to change the password at the configured interval. The maximum number of days the password is valid shall be definable within a range of values of 1 – 500.

e. Either the administrator must change his password at the next login, or the administrator is not forced to change his password at the next login, as configured by the administrator].

6.1.2.15 FIA_UAU.2 User authentication before any action

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

Application Note: *No actions are allowed until the user has logged in (I&A).*

6.1.2.16 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.

Application Note: *No actions are allowed until the user has logged in (I&A).*

6.1.2.17 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [client RADIUS, TACACS+, and local authentication mechanisms] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by the authorised user].

6.1.2.18 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of*] TOE management/administration/security functions listed below to [the Administrator]:

a. Configuring Management Access;

b. Configuring IP CPM Filters;

c. Configuring IPv6 CPM Filters;

d. Configuring CPM Queues;

e. Configuring Password Management Parameters;

f. Configuring Profiles;

g. Configuring Administrators;

h. Copying and Overwriting Administrators and Profiles;

i. Configuring remote administration;

j. Configuring Login control;

k. Configuring RADIUS/TACACS+;

l. Configuring CPU Protection Policies;

m. Configuring SNMP/Syslog;

n. Configuring NTP; and

o. Configuring Event logs.

6.1.2.19 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [UNAUTHENTICATED, AUTHENTICATED and EXPORT SFPs] to restrict the ability to [*change_ default*, *query*, *modify*, *delete*] the security attributes [defined in FDP_IFF.1.1(1), FDP_IFF.1.1(2), and FDP_IFF.1.1(3)] to the [Administrator].

6.1.2.20 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [UNAUTHENTICATED, AUTHENTICATED and EXPORT SFPs] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

6.1.2.21 FMT_SMF.1 Specification of management functions

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

a. start-up and shutdown;

b. create, modify, or delete configuration items;

c. create, delete, empty, and review the audit trail;

d. create, delete, modify, and view filtering rules;

e. perform configuration backups;

f. password management; and

g. security management functions listed in 6.1.2.18 FMT_MOF.1 Management of security functions behaviour.

6.1.2.22 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role~~s~~ [administrators].

FMT_SMR.1.2 The TSF shall be able to associate users with role~~s~~.

6.1.2.23 FPT_ITA.1 Inter-TSF availability with a defined availability metric

FPT_ITA.1.1 The TSF shall ensure the availability of [RADIUS/TACACS+ protocol authentication, authorization data] provided to another trusted IT product within [the constraints of RFCs 2865, 1492 and 2138] given the following conditions [external authentication services are available via either RADIUS, TACACS+, or both, and the TOE has been properly configured for RADIUS/TACACS+ protocol].

Application note: FPT_ITA.1 defines the availability of security parameters exchanged from the TOE to RADIUS/TACACS+ servers (in the Operational environment).

6.1.2.24 EXT_FPT_ITA(1) Inter-TSF availability with a defined availability metric (RADIUS/TACACS+)

EXT_FPT_ITA.1.1(1) The TSF shall ensure the availability of [RADIUS/TACACS+ protocol authentication, authorization data] received from another trusted IT product within [the constraints of RFCs 2865, 1492 and 2138] given the following conditions [external authentication services are available via either RADIUS, TACACS+, or both, and the TOE has been properly configured for RADIUS/TACACS+ protocol].

Application note: EXT_FPT_ITA(1) defines the availability of security parameters exchanged from RADIUS/TACACS servers (in the Operational environment) to the TOE.

6.1.2.25 EXT_FPT_ITA(2) Inter-TSF availability with a defined availability metric (NTP)

EXT_ FPT_ITA.1.1(2) The TSF shall ensure the availability of [NTP data] received from another trusted IT product within [the constraints of RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis] given the following conditions [external NTP server services are available, the TSF has a network connection to a NTP server with a directly-connected device that provides Coordinated Universal Time (UTC), such as a GPS or atomic clock, and the TOE has been properly configured for NTP protocol].

Application note: EXT_FPT_ITA(2) defines the availability of security parameters imported from NTP servers (in the Operational environment) to the TOE.

6.1.2.26 FPT_STM.1 Reliable time stamps (TOE)

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

6.1.2.27 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [administrator defined period of inactivity within a range of 1 to 1440 minutes].

6.1.2.28 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.2.29 FTA_TSE.1(2) TOE session establishment (SAM)

FTA_TSE.1.1 The TSF shall be able to deny remote session establishment based on [maximum number of concurrent remote sessions on the node, values 0 - 15].

6.2 TOE SECURITY ASSURANCE REQUIREMENTS

6.2.1 Overview

The security assurance requirements for the TOE consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Remediation.

6.2.2 Security Assurance Requirements

The assurance components are summarized in the following table:

Assurance Class	Assurance Components	
	Identifier	Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 2 – Security Assurance Requirements (EAL2+)

7 TOE SUMMARY SPECIFICATION

The objective for the TOE summary specification is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. The TOE summary specification should provide the general technical mechanisms that the TOE uses for this purpose. The level of detail of this description should be enough to enable potential consumers to understand the general form and implementation of the TOE.

This section also provides a description of the functions that are carried out by the TOE at the TOE external interfaces (toe Security Functionality Interfaces (TSFI).

This section provides a description of the security functions (and supporting general technical mechanisms) of the TOE that meet the TOE security requirements defined in Section 6. The functions and functional requirements are cross-referenced in Table 7.

7.1 TOE SECURITY FUNCTIONS

7.1.1 Overview

The TOE security functions that were previously introduced are further elaborated in this section. The major functions (e.g., audit) are decomposed to more clearly define their functionality.

7.1.2 F.Audit

7.1.2.1 Audit data generation

The SR OS records the start-up and shutdown of the audit functions.

Log activity of administrators. The SR OS logs the activity of the administrator in a security log.

Log critical network traffic. Applications within the SR OS for which log entries are generated are: IP, routing protocols and services, and CLI and remote access.

Logging of configuration changes. The change activity event source is all events that directly affect the configuration or operation of the TOE as defined in 7.1.4.4.

Security breach logging. The security event source is all events that affect attempts to breach system security such as failed login attempts, attempts to access Management Information Base (MIB) tables to which the administrator is not granted access or attempts to enter a branch of the CLI to which access has not been granted. Security events are generated by the security application.

The SR OS logs the activity of the administrator in a security log. The generating application, a unique event ID within the application, and a short text description is recorded for each applicable event in the audit logs. Event logs are the means of recording system generated events for later analysis. Events are messages generated by applications or processes with the SR OS.

The SR OS is configured to record attempts to breach system security. Logs are configured in the following contexts:

a. Log file — Log files contain log event message streams. Log file IDs are used to direct events, alarms/traps and debug information to their respective targets.
b. SNMP trap groups — SNMP trap groups contain an IP address and community names which identify targets to send traps following specified events.
c. Syslog — Information is sent to a Syslog host that is capable of receiving selected Syslog messages from a network element.
d. Event control — Configures a particular event or all events associated with an application to be generated or suppressed.
e. Event filters — An event filter defines whether to forward or drop an event or trap based on match criteria.
f. Event logs — An event log defines the types of events to be delivered to its associated destination.
g. Event throttling rate — Defines the rate of throttling events.

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The following event sources are the main categories of events that feed the log manager:

a. Security — The security event source is all events that affect attempts to breach system security.
b. Change — The change activity event source is all events that directly affect the configuration or operation of the node.
c. Debug — The debug event source is the debugging configuration that has been enabled on the system.
d. Main — The main event source receives events from all other applications within the SR/ESS-series.

A set of log filter rules is associated with the event log to control which events will be logged in the event log based on combinations of application, severity, event Identification (ID) range, and the subject of the event.

An event log within the SR OS associates the event sources with logging destinations:

a. Memory - All selected log events will be directed to an in-memory storage area. A memory log is a circular buffer. When the log is full, the oldest entry in the log is replaced with the new entry. When a memory log is created, the specific number of entries it holds is specified; otherwise it will assume a default size. An event log sends entries to a memory log destination.
b. Session - An administrator logged in to the local console device or connected to the CLI via a remote session also creates a log with a destination type of 'session'. Events are displayed to the session device until the administrator logs off. When the administrator logs off, the 'session' type log is deleted. A session destination is a temporary log destination which directs entries to the active session for the duration of the session. When the session is

terminated, for example, when the administrator logs out, the event log is removed. Event logs configured with a session destination are not stored in the configuration file. Event logs direct log entries to the session destination.

c. SNMP traps - Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in Notification Log- Management Information Base (MIB) tables.
d. Syslog - All selected log events are sent to the Syslog address.
e. File - All selected log events will be directed to a file on one of the CPM’s compact flash disks. Log files are used by event logs and are stored on the compact flash devices in the file system. A log file is identified with a single log file ID, but a log file will generally be composed of a number individual files in the file system. Log files are created in specific subdirectories with standardized names in accordance with on the type of information stored in the log file.

Only a single log destination is associated with an event log. An event log is associated with multiple event sources, but it only has a single log destination.

An event log has the following properties:

a. A unique log ID. The log ID is a short, numeric identifier for the event log. A maximum of ten logs are configured at a time.
b. One or more log sources. The source stream or streams to be sent to log destinations are specified. The source must be identified before the destination is specified. The events are from the main event stream, events in the security event stream, or events in the administrator activity stream.
c. One event log destination. A log only has a single destination. The destination is one of console, session, Syslog, SNMP-trap-group, memory, or a file on the local file system.
d. Optional events filter policy. A set of event filter rules defines whether to forward or drop an event or trap based on match criteria. The log manager uses event filter policies to allow fine control over which events are forwarded or dropped. Like other policies with the SR OS, filter policies have a default action. The default actions are either: Forward, or Drop.

Log entries that are forwarded to a destination are formatted in a way appropriate for the specific destination whether it be recorded to a file or sent as an SNMP trap, but log event entries have common elements or properties:

a. A time stamp in Universal Time Co-ordinated (UTC) or local time;
b. The generating application;
c. A unique event ID within the application;
d. A router name identifying the VRF-ID that generated the event;
e. A subject identifying the affected object; and
f. A short text description.

7.1.2.2 User identity association

For audit events resulting from actions of identified administrators, the SR OS is able to associate each auditable event with the identity of the administrator that caused the event.

7.1.2.3 Audit review

The administrator reads all the information in the log destinations (i.e., SNMP-trap-group, memory, or a file on the local file system) via CLI log detail commands.

Log Commands are in the following categories: Configuration Commands, Show Commands, and Clear Commands.

The LOG-ID command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log. If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics. If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed. Contents of logs with console, session or syslog destinations cannot be displayed. The actual events are only be viewed on the receiving syslog or console device (part of the OE).

The administrator limits the number of log entries displayed to the number specified, and displays only events generated by the specified application or the specified and higher severity (cleared, indeterminate, critical, major, minor, warning). The administrator displays the log entry numbers from a particular entry sequence number to another sequence number. If the to-sequence number is not provided, the log content to the end of the log is displayed.

Logs are normally shown from the newest entry to the oldest in descending sequence number order on the screen. When using the ascending parameter, the log will be shown from the oldest to the newest entry.

The log files are stored in system memory on compact flash (cf1: or cf2:) in a compressed (tar) XML format and are retrieved using file-copy. The SR OS creates two directories on the compact flash to store the files.

When a log file is created, only the compact flash device for the log file is specified. Log files are created in specific subdirectories with standardized names depending on the type of information stored in the log file. Event log files are always created in the \log directory on the specified compact flash device. The \act-collect directory is where active logs are written. When a log is rolled over, the active file is closed and archived in the \act directory before a new active log file created in \act-collect. Logging policies are used to ensure that different level events are send to different logging destinations.

The SR OS provides authorized administrators with the capability to read audit data from the audit records in a manner suitable for the administrator to interpret the information by means of the CLI SHOW LOG command which displays the following information:

a. applications;
b. event-control;
c. file-id;
d. filter-id;
e. log-collector;
f. log-id;
g. snmp-trap-group; and
h. syslog [syslog-id].

The administrator executes the following log commands:

a. Configuration Commands;
b. Generic Commands;
c. Event Control;
d. Log File Commands;
e. Log Filter Commands;
f. Log Filter Entry;
g. Log Filter Entry Match Commands;
h. Syslog Configuration Commands;
i. SNMP Trap Groups;
j. Logging Destination Commands;
k. Show Commands; and
l. Clear Commands.

The administrator shows log collector statistics for the main, security, change and debug log collectors.

The administrator displays event file log information. A summary output of all event log files is displayed along with detailed information on the event file log.

The administrator reinitializes/rolls over the specified memory/file. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by log clear command.

7.1.2.4 Restricted Audit review

Administrator capabilities are all controlled via the configuration of the administrator profile. This profile allows a administrator's permissions to allow or disallow access to any command in the system's management down to the granularity of an individual command.

The SR OS prohibits all administrators read access to the audit records, except those administrators that have been granted explicit read-access. This is accomplished by means of administrator profiles that are used to deny or permit access to a CLI hierarchical branch or specific commands, including the log clear command.

7.1.3 F.I&A

7.1.3.1 Authentication failure handling (console)

The following is defined by the administrator: (1) The number of unsuccessful login attempts allowed for the specified time. (2) The period of time, in minutes, that a specified number of unsuccessful attempts that are made before the administrator is locked out. (3) The lockout period in minutes where the administrator is not allowed to login. When the administrator exceeds the attempted count times in the specified time, then that administrator is locked out from any further login attempts for the configured time period.

Parameters are modifiable from the provided default values:

a. The SR OS detects when an administrator configurable positive integer (default: 3, within a range of values 1 – 64), within an administrator configurable period of time (default 5 minutes, and within a range of values 0 — 60)], unsuccessful authentication attempts occurs related to any claimed administrator ID attempting to authenticate to the SR OS via the console.

b. When the defined number of unsuccessful authentication attempts has been met, the SR OS will at the option of the Administrator prevent activities that require authentication until an action is taken by the Administrator, or until an Administrator defined time period (default: 10 minutes and within a range of values 0 - 1440 minutes) has elapsed.

7.1.3.2 Authentication failure handling (exponential backoff)

The exponential-back off parameter enables the exponential-back off of the login prompt. This function is used to deter dictionary attacks, when a malicious administrator trys to gain access to the SR OS by using a script to try any conceivable password. SR OS increases the delay between login attempts exponentially to mitigate attacks. It is applied to the console login.

The SR OS shall detect when [one (1)], within [an administrator configurable period of time, (default 5 minutes, and within a range of values 0 – 60 minutes)], unsuccessful authentication attempts occurs related to [any claimed administrator ID attempting to authenticate to the SR OS via the local Console].

7.1.3.3 Verification of secrets

The verifications of secrets applies to all authentication methods: local console, and RADIUS and TACACS+.

The password needs to satisfy the following requirements:

a. A minimum length (characters) default 6 and within a range of 1-8,
b. A maximum length of up to 20 characters if unhashed, and 32 characters if hashed;
c. at least one upper and one lower case character;
d. at least one numeric character must be present in the password; and
e. at least one special character must be present in the password. Special characters include: ~!@#$%^&*()_+|{}:"<>?`-=\[];',./.

Also, as part of administrator registration, the following are set:

a. Y - administrator must change his password at the next login; or
b. N - The administrator is not forced to change his password at the next login.

Definitions are:

a. numeric — Specifies that at least one numeric character must be present in the password. This keyword is used in conjunction with the mixed-case and special-character parameters.
b. special-character — Specifies that at least one special character must be present in the password. This keyword is used in conjunction with the numeric and special-character parameters.
c. Special characters include: ~!@#$%^&*()_+|{}:"<>?`-=\[];',./.
d. mixed-case — Specifies that at least one upper and one lower case character must be present in the password. This keyword is used in conjunction with the numeric and special-character parameters.

7.1.3.4 User authentication before any action

The SR OS is configured to use RADIUS, TACACS+, and local/remote authentication to validate administrators requesting access to the network. The order in which password authentication is processed among RADIUS, TACACS+ and local passwords is specifically configured.

Authentication validates a administrator name and password combination when a administrator attempts to log in. When an administrator attempts to log in through the console, or remotely, the SR-Series or ESS-Series client sends an access request to a RADIUS, TACACS+, or local database.

7.1.3.5 User identification before any action

The SR OS validates an administrator name and password combination when a administrator attempts to log in.

7.1.3.6 Multiple authentication mechanisms

The SR OS implements local, RADIUS, and TACACS+ authentication to control the actions of specific administrators by applying a profile based on administrator name and password configurations.

7.1.4 F.Security Management

7.1.4.1 Management of security functions behaviour

Administrator capabilities are all controlled via the configuration of the administrator profile. This profile allows a administrator's permissions to allow or disallow access to any command in the system's management down to the granularity of an individual command. The following security functions are restricted to the administrators.

The administrator will perform the following:

a. Configures authentication failure handling configurable integer of unsuccessful authentication attempts within configurable range of time, and configurable lock out period of time that occurs related to a administrator's authentication.

b. Controls when (e.g., time and day(s) of the week) and where (e.g., from a specific network address) administrators, and authorized IT entities access the TOE.

c. Configures the maximum number of active sessions.

d. Configures IP/MAC CPM filters and queues that control all traffic going in to the CPM, including all routing protocols.
e. Configures authentication attempts count, time interval [minutes], and lockout time period [minutes];
f. Configures authentication-order for local console, RADIUS and TACACS+;
g. Configures password complexity [numeric] [special-character] [mixed-case];
h. Configures password minimum-length value.
i. Configures: management access filters, profiles, administrator access parameters, password management parameters.
j. Enables RADIUS and/or TACACS+ (TOE client-side).
k. Configures event and logs.
l. Configures access parameters for individual administrators - the login name for the administrator and information that identifies the administrator.
m. Configures administrator profiles used to deny or permit access to CLI command tree permissions, or specific CLI commands.
n. Copies a profile or administrator or overwrite an existing profile or administrator.
o. Allows/disallows a administrator the privilege to change their password for console login.

The administrator will also configure the following SNMP access group information:
a. Group name - The access group name.
b. Security model - The security model required to access the views configured in this node.
c. Security level - Specifies the required authentication and privacy levels to access the views configured in this node.

d. Read view - Specifies the variable of the view to read the MIB objects.
e. Write view - Specifies the variable of the view to configure the contents of the agent.
f. Notify view - Specifies the variable of the view to send a trap about MIB objects.

The administrator will execute the following security CLI commands

a. Configuration Commands;
b. General Security Commands;
c. Login, Telnet, remote management commands;
d. Management Access Filter Commands;
e. Password Commands;
f. Profile Management Commands;
g. Administrator Management Commands;
h. RADIUS Client Commands;
i. TACACS+ Client Commands;
j. Generic 802.1x Commands;
k. CPM Filter Commands;
l. CPM Queue Commands;
m. TTL Security Commands;
n. CPU Protection Commands;
o. Show Commands;
p. Security Commands;
q. Login Control;
r. Clear Commands;
s. Authentication Commands;
t. CPM Filter Commands;
u. CPU Protection Commands; and
v. Debug Commands.

The administrator will perform the following logging tasks:

a. Modify a Log File;
b. Delete a Log File;
c. Modify a File ID;
d. Delete a File ID;
e. Modify a Syslog ID;
f. Delete a Syslog;
g. Modify an SNMP Trap Group;
h. Delete an SNMP Trap Group;
i. Modify a Log Filter;
j. Delete a Log Filter;
k. Modify Event Control Parameters; and
l. Return to the Default Event Control Configuration.

7.1.4.2 Management of security attributes

Simple security attributes (unauthenticated policy)

The administrator specifies information flow policy rules (i.e., routing protocols and ingress/egress traffic filtering and peer filtering) that contain information security attribute values, and associate with that rule an action that permits the information flow or disallows the information flow. When a packet arrives at the source interface, the information security attribute values of the packet are compared to each information flow policy rule and when a match is found the action specified by that rule is taken.

Subject and information security attributes used are:

a. IP network address and port of source subject;
b. IP network address and port of destination subject;
c. transport layer protocol and their flags and attributes (UDP, TCP);
d. network layer protocol (IP, ICMP);
e. Documented Special Use (DUSA) IPv4 addresses;
f. interface on which traffic arrives and departs; and
g. routing protocols and their configuration and state.

Simple security attributes (authenticated policy)

The Administrator using CLI syntax:

a. configures administrator name/password and profile;
b. configures local home directory for console and remote access;
c. grants a administrator permission for remote or console access;
d. configures the maximum number of concurrent inbound remote sessions; and
e. configures idle timeout for file-copy, console, or remote sessions which determines when the session is terminated by the system.
f. Configures Management Access Filters to control all traffic in and out of the SR OS and to restrict management of the SR OS by other nodes outside either specific (sub)networks or through designated ports.

Subject and information security attributes used are:

a. Source subject security attributes: source port and IP protocol ID and address, username/password and profile, source network identifier, remote or console session idle timeout, maximum number of concurrent inbound remote sessions, administrator permission for remote or console access, local home directory for the administrator for remote or console access;
b. Destination subject security attributes: set of destination subject identifiers (UDP/TCP port number); and
c. Information security attributes: authenticated identity of source subject; identity of destination subject; transport layer protocol; and destination subject service identifier (TCP destination port number).

Application Note: "Service identifier" specifies a service that is above the network and transport layers in the protocol stack.

Simple security attributes (export policy)

The event log is configured to send events to one syslog destination. Syslog destinations have the following properties:

a. Syslog server IP address.
b. The UDP port used to send the syslog message.
c. The Syslog Facility Code (0 - 23) (default 23 - local 7).
d. The Syslog Severity Threshold (0 - 7) - events exceeding the configured level will be sent.

The Administrator configures a Syslog Target using CLI syntax to configure a syslog file. Log events cannot be sent to a syslog target host until a valid syslog ID exists. All references to the syslog ID must be deleted before the syslog ID can be removed.

The Administrator uses CLI syntax to configure the port number to receive SNMP request messages and to send replies.

Subject and information security attributes used are:

a. [Source subject security attributes: source network identifier; and
b. Destination subject security attributes:
   i) Set of destination network identifiers;
   ii) Syslog server IP address;
   iii) UDP port used to send the syslog message;
   iv) Syslog Facility Code;
   v) Syslog Severity Threshold;
   vi) Port number used to send SNMP traffic.

7.1.4.3 Static attribute initialization

SR OS equipped systems arrive out-of-the-box configured with no services turned on and with direct console access only. In addition, no IP address is configured on the router by default. This requires physical or out-of-band console access in order to bring a new system up. The SR OS requires local console access to initially configure an IP address and enable remote access.

Administrators are setup with an individual account configured to only allow the minimum access to perform the assigned support duties. The administrator is instructed in administrative guidance how to set and specify alternative initial default attribute values.

7.1.4.4 Specification of management functions

The Administrator performs the following security management functions on the SR OS:

a. start-up and shutdown;
b. create, modify, or delete configuration items;
c. modify and set the time and date;

d. create, delete, empty, and review the audit trail;
e. create, delete, modify, and view filtering rules;
f. perform configuration backups;
g. password management;
h. security management functions listed in 7.1.4.1 Management of security functions behaviour.

Password management parameters consists of defining aging, the authentication order and authentication methods, password length and complexity, as well as the number of attempts a administrator enters a password. Also, as part of administrator registration, the following are set:

a. Y — The administrator has the ability to change the login password.
b. N — The administrator does not have the ability to change the login password

The SR OS implements the periodic backup of the SR OS configurations. The backups are used for recovering the network configurations when major network events happen, such as hardware failure and misconfigurations.

For additional management functions refer to section 7.1.4.1.

7.1.4.5 Security roles

The SR OS allows all authorized administrators with the needed authority to configure and control the associated features.

Only authenticated administrators and administrators are permitted to use or manage the router resources. There is one roles associated with the SR OS –ADMINISTRATOR role. Only administrators are permitted to use or manage the router resources.

Only authenticated administrators execute certain CLI commands. Authorization features allow administrators to configure administrator profiles which are used to limit what CLI commands are executed by the specific authenticated administrator.

Once an administrator has been authenticated the SR OS is configured to perform authorization.

Profiles consist of a suite of commands that the administrator is allowed or not allowed to execute. When an administrator issues a command, the SR OS looks at the command and the administrator information and compares it with the commands in the profile. If the administrator is authorized to issue the command, the command is executed. If the administrator is not authorized to issue the command, then the command is not executed.

7.1.5 F.TOE Access

7.1.5.1 TSF-initiated termination

The SR OS allows configuring login control parameters for console and remote administration sessions.

The SR OS has the ability to terminate stale connections. The SR OS terminates interactive session after an administrator defined period of inactivity with a default value of 30 minutes, and within a range of 1 to 1440 minutes]

This idle-time parameter configures the idle timeout for console, or remote sessions before the session is terminated by the system. This would reduce the chance for the unauthorized administrators to access the router through an unattended opened session. By default, an idle console, or remote session times out after thirty (30) minutes of inactivity. This timer is set per session.

7.1.5.2 User-initiated termination.

Administratiors initiate termination of their own sessions. The SR OS allows a administrator to terminate their own session by issuing the command “logout” at the CLI prompt.

7.1.5.3 TOE session establishment

The SR OS will deny session establishment after an administrator defined number of active SAM sessions thereby limiting the number of inbound SAM sessions. The SR OS denies remote session establishment based on maximum number of concurrent remote sessions on the node, default 5, values 0 - 15].

7.1.6 F.User data protection

7.1.6.1 Export of administrator data with security attributes

The SR OS as Out-of-band (OOB) and In-band (IB) export functions (i.e., Syslog, SNMP). Logging policies ensure that different level events are sent to different logging destinations. Minor events are sent to a file destination or Syslog server and critical events are sent to SNMP trap host for immediate action. The SR OS also exports RADIUS or TACACS+ audit data which includes the associated node, user and timestamp for all events executed by a given administrator.

7.1.6.2 Subset information flow control (unauthenticated policy)

The TOE enforces an UNAUTHENTICATED SFP whereby the network packets sent through the TOE are subject to router information flow control rules setup by the administrator.

All subsystems are involved in determining how a packet will be forwarded and or performing the packet forwarding process. The controlling mechanisms include the system configuration, protocol state for the forwarding of the actual data.

7.1.6.3 Subset information flow control (authenticated policy)

The TOE enforces an AUTHENTICATED SFP whereby information is passed via application proxy (Console, SAM). Administrators must first be granted access by the administrator and then authenticated in order to access the router by Console, SAM.

The TOE will only send and accept management connections from properly configured or authenticated sources.

7.1.6.4 Subset information flow control (export policy)

The TOE enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap and Syslog destinations.

The TOE will only send management data to properly configured destinations.

7.1.6.5 Simple security attributes (unauthenticated policy)

The TOE uses traffic filters and protocol configuration and protocol state to enforce the UNAUTHETICATED SFP.

The administrator configures the SR-Series routers and ESS-Series switches setting the following protocols, standards, and services from the set of: OSPFv2, IS-IS, BGP-4, MPLS (LDP, RSVP-TE). TCP/IP stack is implemented as a common protocol stack for IP, UDP and TCP communications. That packets going to the TOE are first classified into forwarding classes (FCs).

Filter policies, also referred to as Access Control Lists (ACLs), are templates applied to services or network ports to control network traffic into (ingress) or out of (egress) a service access port or network port based on IP, IPv6, and MAC matching criteria. Filters are applied to services to look at packets entering or leaving a SAP or network interface. Filters can be used on several interfaces. The same filter can be applied to ingress traffic, egress traffic, or both. Ingress filters affect only inbound traffic destined for the routing complex, and egress filters affect only outbound traffic sent from the routing complex.

Access Control Lists provide complete control over the traffic which is allowed to enter the network. The SR OS routes the traffic that is permitted by the information flow policies. All traffic passing through the router is processed by the ACL attached to the interface/ protocol. An ACL is filter policy applied on ingress or egress to a SAP on an interface to control the traffic access. The ACL prevents an unknown party (identified by IP match or Media Access Control (MAC) match criteria) to access the router/switch’s infrastructure and service layer, and provide security protections of both layers. The ACL is processed top-down, with processing continuing until the first match is made. All traffic that successfully clears the ACLs is processed by the routing tables. The routing table is processed top-down, with processing continuing until the first match is made. The routing table may be statically updated by a privileged administrator or dynamically through routing protocols.

Dedicated CPM hardware queues are also allocated for certain traffic designated to the CPUs and set the corresponding rate-limit for the queues. These filters drop or accept packets, as well as allocate dedicated hardware shaping queues for traffic directed to the control processors. CPM filters and queues control all traffic going in to the CPM, including all routing protocols. They apply to packets from all network and access ports, but not to packets from a management Ethernet port.

The administrator specifies information flow policy rules (routing protocols and ingress/egress traffic filtering and peer filtering) that contain information security attribute values, and associate with that rule an action that permits the information flow or disallows the information flow. When a packet arrives at the source interface, the information security attribute values of the packet are compared to each information flow policy rule and when a match is found the action specified by that rule is taken. The set of identifiers are associated with the physical router interfaces.

Subject and information security attributes used are:

a. IP network address and port of source subject;
b. IP network address and port of destination subject;
c. transport layer protocol and their flags and attributes (UDP, TCP);
d. network layer protocol (IP, ICMP);
e. Documented Special Use (DUSA) IPv4 addresses;
f. interface on which traffic arrives and departs; and
g. routing protocols and their configuration and state.

IP/MAC filter policies match criteria that associate traffic with an ingress or egress SAP. A filter policy compares the match criteria specified within a filter entry to packets coming through the system, in the order the entries are numbered in the policy. When a packet matches all the parameters specified in the entry, the system takes the specified action to either drop or forward the packet. If a packet does not match the entry parameters, the packet continues through the filter process and is compared to the next filter entry, and so on. If the packet does not match any of the entries, then system executes the default action specified in the filter policy. Each filter policy is assigned a unique filter ID.

When filter rule entries are created, they are arranged sequentially from the most explicit entry to the least explicit. Filter matching ceases when a packet matches an entry. The entry action is performed on the packet. The TOE performs either drop or forward action. To be considered a match, the packet must meet all the conditions defined in the entry. Packets are compared to entries in a filter policy in an ascending entry ID order.

When a filter consists of a single entry, the filter executes actions as follows:

a. If a packet matches all the entry criteria, the entry’s specified action is performed (drop or forward); and
b. If a packet does not match all of the entry criteria, the policy’s default action is performed.

If a filter policy contains two or more entries, packets are compared in ascending entry ID order:

a. Packets are compared with the criteria in the first entry ID.

b. If a packet matches all the properties defined in the entry, the entry's specified action is executed.
c. If a packet does not completely match, the packet continues to the next entry, and then subsequent entries.
d. If a packet does not completely match any subsequent entries, then the default action is performed.

TTL security parameters are used for incoming packets. BGP/LDP accepts incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value (values 1 — 255) configured for that peer. A link-specific rate is also used for CPU protection. This limit shall be applied to all interfaces within the system. The CPU will receive no more than the configured packet rate for all link level protocols.

The SR OS provides automatic detection of attacks triggered by excessive control plane and routing protocol traffic, and it recognizes signatures of some common Distributed and other DoS (D/DoS) attacks and further it will suppress these attacks using the ACLs.

7.1.6.6 Simple security attributes (authenticated policy)

The TOE also enforces an AUTHENTICATED SFP whereby information is passed via application proxy (Console, SSH, file-copy). Users must first be granted access by the administrator and then authenticated in order to access the router by Console, SSH, file-copy.

Source subject security attributes are: source port and IP protocol ID and address, username/password and profile, source network identifier, remote or console session idle timeout, maximum number of concurrent inbound remote sessions, administrator permission for remote or console access, local home directory for the administrator for remote or console access. Destination subject security attributes are: set of destination subject identifiers (UDP/TCP port number).

Any packet that is destined to the SR OS, has to have the correct MAC address, and IP address that has been assigned by the network operator to be able to remotely operate the SR OS. Once the packet has been identified to be forwarded to the CPM, it is put under the influence of the CPM filters.

Management Access Filters (MAFs) control all traffic to the CPM as well as all routing protocols. These filters apply to packets from all ports to restrict management of the SR OS from other nodes who are unauthorized. MAFs restricts access to the SR OS to small list of SAM servers or support workstations. MAFs control all traffic going into the CPM, including all routing protocols. They apply to packets from all ports. The filters are used to restrict management of the SR router or ESS switch by other nodes outside either specific (sub)networks or through designated ports. By default, there are no filters associated with security options. The MAF and entries must be explicitly created on each router. These filters apply to the management Ethernet port. MAFs are used to restrict traffic on OOB Ethernet port. When the first match is found actions are executed. Entries must be sequenced correctly from most to least explicit.

7.1.6.7 Simple security attributes (export policy)

The TOE also enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap and Syslog destinations.

Subject and information security attributes used are:

a. [Source subject security attributes: source network identifier; and
b. Destination subject security attributes:
   i) Syslog server IP address;
   ii) UDP port used to send the syslog message;
   iii) Syslog Facility Code;
   iv) Syslog Severity Threshold;
   v) Set of destination network identifiers;
   vi) IP address of the SNMP trap receiver;
   vii) UDP port used to send the SNMP trap;
   viii) SNMPv3 used to format the SNMP notification; and
   ix) Security name and level for SNMPv3 trap receivers.

For SNMP traps sent out-of-band through the Management Ethernet port, the source IP address of the trap is the IP interface address defined on the Management Ethernet port. For SNMP traps sent in-band, the source IP address of the trap is the system IP address of the SR OS.

Each trap target destination of a trap group receives the identical sequence of events as defined by the log ID and the associated sources and log filter applied.

The Syslog protocol is used to convey event notification messages. Parameters are defined identified in RFC 5424 *The Syslog Protocol* which describes the format of a Syslog message.

7.1.7 F.TSF_Protection

The SR OS ensures the availability of security parameters exchanged to/from the TOE to RADIUS/TACACS+ servers (in the Operational environment).

The SR OS ensures the availability of security parameters imported from NTP servers (in the Operational environment) to the TOE.

7.1.8 F.Console_Access

The SR OS has a direct connection via the physical RS232 console interface and a remote console connection to perform security management functions. This interface is controlled via an information flow control (authenticated policy) as defined herein. The SR OS requires local access to initially configure. Local console authentication access via a RS-232 port to the router uses administrator names and passwords to authenticate login attempts.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 Threats and TOE Security Objectives

Table 3 provides a bi-directional mapping of Security Objectives to Threats. It shows that each of the threats is addressed by at least one of the objectives, and that each of the objectives addresses at least one of the threats.

	O.AUDIT	O.MANAGE	O.I&A	O.MEDIATE	O.TOE_ACCESS
T.AUDIT	X				
T.TSF_DATA		X			
T.MEDIATE				X	
T.UNATTENDED_SESSION					X
T.UNAUTH_MGT_ACCESS			X		

Table 3 - Mapping of Security Objectives to Threats

T.AUDIT	*Actions performed by administrators (modification of TOE and network infrastructure and service layer system security configuration/parameters) may not be known to the administrators due to actions not being recorded (and time stamped) or the audit records not being reviewed prior to the machine shutting down, or an unauthorized administrator modifies or destroys audit data.* The O.AUDIT objective requires that the TOE mitigate this threat by generating audit records. O.AUDIT requires the TOE provide the Authorized administrator with the capability to view Audit data. O.AUDIT requires that the TOE protect audit data. O.AUDIT also requires the TOE to restrict audit review to administrators who have been granted explicit read-access. The OE.ADMINISTRATOR objective on the environment assists in covering this threat on the TOE by requiring that the administrator abide by the instructions provided by the TOE documentation, including the administrator guidance to periodically check the audit record. The OE.TIME objective on the environment assits in covering this threat by requiring that the OE provide accurate time to the TOE for use in the audit records. These objectives provide complete TOE coverage of the threat.

T.TSF_DATA	*A malicious user may gain unauthorised access to inappropriately view, tamper, modify, or delete TOE Security Function (TSF) data.* The O.MANAGE objective requires that the TOE mitigate this threat by providing 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 objective provides complete TOE coverage of the threat. The OE.ADMINISTRATOR objective on the environment assists in covering this threat on the TOE by requiring that the administrator abide by the instructions provided by the TOE documentation, including the administrator guidance to periodically check the audit record, reducing the possibility for error.
T.MEDIATE	*An unauthorized entity may send impermissible information through the TOE which results in the exploitation (e.g., destruction, modification, or removal of information and/or other resources), and/or exhaustion of resources on the network (e.g. bandwidth consumption or packet manipulation).* The O.MEDIATE security objective requires that the TOE mitigate this threat by ensuring all information that passes through the network is mediated by the TOE. O.MEDIATE requires that the TOE mitigate this threat by mediating 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 objective provides complete TOE coverage of the threat.

T.UNATTENDED_SESSION

A administrator may gain unauthorized access to an unattended session and view and change the TOE security configuration.

The O. TOE_ACCESS objective requires that the TOE mitigate this threat by including mechanisms that place controls on administrator's sessions. Local and remote administrator's sessions are dropped after an Administrator-defined time period of inactivity. Dropping the connection of a local and remote session (after the specified time period) reduces the risk of someone accessing the local and remote machines where the session was established, thus gaining unauthorized access to the session.

This objective provides complete TOE coverage of the threat.

T.UNAUTH_MGT_ACCESS

An unauthorized administrator gains management access to the TOE and views or changes the TOE security configuration.

The O.I&A objective requires that the TOE mitigate this threat by uniquely identifying and authenticating the claimed identity of all administrators before granting management access and to control their actions. O.I&A requires a administrator to enter a unique identifier and authentication before management access is granted. O.TRUSTED_PATH ensures that the local console access is secure.

These objectives provide complete TOE coverage of the threat.

8.1.2 Assumptions and OSPs and Operational environment Objectives

Table 4 provides a bi-directional mapping of Assumptions to Security Objectives for the Operational environment. Since the Security Objectives for the Operational environment were derived directly from the Assumptions there is a one to one mapping between them. It is also clear since the Security Objectives for the Operational environment are simply a restatement of the applicable assumption, that each objective is suitable to meet its corresponding assumption.

	OE.ADMINISTRATOR	OE.GENPURPOSE	OE.CONNECTIVITY	OE.EXT_AUTHORIZATION	OE.LOCATION	OE.PHYSICAL	OE.INTEROPERABILITY	OE.TIME	OE.TRUSTED_PATH/CHANNEL	OE.DEPLOYED_CONFIG	OE.USERS	OE.CONSOLE
A.ADMINISTRATOR	X											
A.GENPURPOSE		X										
A.CONNECTIVITY			X									
A.EXT_AUTHORIZATION				X								
A.LOCATION					X							
A.PHYSICAL						X						
A.INTEROPERABILITY							X					
A.TIMESTAMP								X				
A.TRUSTED PATH/CHANNEL									X			
P.DEPLOYED_CONFIG										X		
P.USERS											X	
P.CONSOLE												X

Table 4 - Mapping of Assumptions to Security Objectives for the Operational Environment

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Security Functional Requirements Rationale

Table 5 provides a bi-directional mapping of Security Functional Requirements to TOE Security Objectives. Table 5 demonstrates that each of the applicable objectives for the TOE is addressed by at least one of the functional requirements and that each of the functional requirements address at least one of the objectives.

The table is followed by a discussion of how each applicable Security Objective is addressed by the corresponding Security Functional Requirements. It should be noted that some of the TOE Security Objectives are satisfied by Assurance Requirements rather than Functional Requirements. These objectives are discussed in Section 8.2.3.

	O.AUDIT	O.MANAGE	O.I&A	O.MEDIATE	O.TOE_ACCESS
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FDP_ETC.2		X		X	
FDP_IFC.1(1)				X	
FDP_IFC.1(2)				X	
FDP_IFC.1(3)				X	
FDP_IFF.1(1)				X	
FDP_IFF.1(2)				X	
FDP_IFF.1(3)				X	
FIA_AFL.1(1)			X		

	O.AUDIT	O.MANAGE	O.I&A	O.MEDIATE	O.TOE_ACCESS
FIA_AFL.1(2)			X		
FIA_SOS.1			X		
FIA_UAU.2			X		
FIA_UID.2			X		
FIA_UAU.5			X		
FMT_MOF.1		X			
FMT_MSA.1		X			
FMT_MSA.3		X		X	
FMT_SMF.1		X			
FMT_SMR.1		X			
FPT_ITA.1			X		
EXT_FPT_ITA.1(1)			X		
EXT_FPT_ITA.1(2)	X				
FTA_SSL.3					X
FTA_SSL.4					X
FTA_TSE.1(2)					X

Table 5 - Mapping of Security Functional Requirements to TOE Security Objectives

O.AUDIT

The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event. The TOE will provide the privileged administrators the capability to review Audit data

	and will restrict audit review to administrators who have been granted explicit read-access. The TOE will also protect audit data. The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event. [FAU_GEN.1 and FAU_GEN.2]. The TOE will provide the privileged administrators the capability to review Audit data. [FAU_SAR.1and FAU_SAR.2]. The TOE will ensure the availability of [NTP data] received from another trusted IT product within [the constraints of RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis] given the following conditions [external NTP server services are available, the TSF has a network connection to a NTP server with a directly-connected device that provides Coordinated Universal Time (UTC), such as a GPS or atomic clock, and the TOE has been properly configured for NTP protocol].
O.MANAGE	*The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.* The TOE is required to provide the ability to restrict the use of TOE management/administration/security functions to authorized administrators of the TOE [FMT_MOF.1]. The TOE will capable of performing security management functions. The TOE is capable of performing numerous management functions including start-up, shutdown, and creating/modifying/deleting configuration items [FMT_SMF.1]. The TOE must be able to recognize the administrative role that exists for the TOE [FMT_SMR.1]. The TOE must restrict the ability to manage security attributes associated with the UNAUTHENTICATED SFP to the administrator. [FMT_MSA.1] The TOE must allow the privileged administrator to specify alternate initial values when an object is created. [FMT_MSA.3]. The TOE ensures that all administrator actions resulting in the access to TOE security functions and configuration data are

	controlled. [FMT_SMF.1, FMT_FMT_MOF.1] The TOE ensures that access to TOE security functions and configuration data is based on the assigned administrator role. [FMT_SMR.1] TOE ensures that the management functions are available via console access and other OOB & IB functions (i.e., syslog, SNMP). [FDP_ETC.2]
O.I&A	*The TOE will uniquely identify and authenticate the claimed identity of all administrative administrators before granting management access and to control their actions.* The TOE must uniquely identify and authenticate the claimed identity of all administrative administrators before granting management access. Administrators authorized to access the TOE must be defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Before anything occurs on behalf of the administrator, the administrator’s identity is identified to the TOE [FIA_UID.2]. Multiple consecutive unsuccessful attempts to authenticate result in locking of the account until the authentication administrator re-enables it [FIA_AFL.1(1) and (2)]. The TOE must increase the delay between login attempts exponentially after each failed login attempt. The TOE must also check passwords for aging, minimum length, login attempts, and complexity [FIA_SOS.1]. The TOE must provide RADIUS, TACACS+, and local authentication mechanisms to support administrator authentication. The TOE must ensure the availability of RADIUS/TACACS+ protocol authentication data provided to or received from another trusted IT product within the constraints of RFCs 2865, 1492 and 2138 provided that external authentication services are available via either RADIUS, TACACS+, or both, and the TOE has been properly configured for RADIUS/TACACS+ authentication protocol. [FPT_ITA.1, EXT_FPT_ITA(1)]
O.MEDIATE	*The TOE must mediate the flow of all information between hosts located on disparate internal and external networks governed by the TOE. The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.* The TOE is required to identify the entities involved in the

	unauthenticated information flow control SFP [FDP_IFC.1 and FDP_IFC.2] and to identify the attributes of the administrators sending and receiving the information in the unauthenticated, unauthenticated and export SFPs [FDP_IFF.1(1), FDP_IFF.1(2), and FDP_IFF.1(3),]. The policy is defined by saying under what conditions information is permitted to flow [FDP_IFF.1]. Information that is permitted to flow will then be routed according to the information in the routing table [FDP_IFF.1]. The TOE ensures that there is a default deny policy for the information flow control security rules [FMT_MSA.3]. The TOE ensures that the export of user data is controlled. [FDP_ETC.2]
O.TOE_ACCESS	*The TOE will provide mechanisms that control a administrator's logical access to the TOE and to explicitly deny access to specific administrators when appropriate.* The TOE will terminate an interactive session after an administrator defined time interval of administrator inactivity. [FTA_SSL.3] The administrator is also able to terminate their own interactive session. [FTA_SSL.4] The TOE will deny session establishment after an administrator defined number of active SAM sessions. [FTA_TSE.1. This requirement limits the number of inbound SAM sessions.

8.2.2 Assurance Requirements Rationale

Alcatel-Lucent has decided that the TOE will be evaluated at EAL2, augmented with flaw remediation. This combination is termed EAL2+. This provides a level of independently assured security that is consistent with the postulated threat environment. Specification of EAL2+ includes the vulnerability assessment component.

8.2.3 Functional Requirement Dependencies Rationale

8.2.3.1 Dependency Analysis

Table 6 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency. Justification for any dependencies which are not satisfied is listed at the end of Table 10.

SFR Identifier	Name	Dependency	Dependency Met
FAU_GEN.1	Audit data generation	FPT.STM.1	Y, OE objective
FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1	Y
FAU_SAR.1	Audit review	FAU_GEN.1	Y
FAU_SAR.2	Restricted audit review	FAU_SAR.1	Y
FDP_ETC.2	Export of user data with security attributes	FDP_IFF.1(3)	Y
FDP_IFC.1(1)	Subset information flow control (unauthenticated policy)	FDP_IFF.1(1)	Y
FDP_IFC.1(2)	Subset information flow control (authenticated policy)	FDP_IFF.1(2)	Y
FDP_IFC.1(3)	Subset information flow control (export policy)	FDP_IFF.1(3)	Y
FDP_IFF.1(1)	Simple security attributes (unauthenticated policy)	FDP_IFC.1(1)	Y
FDP_IFF.1(2)	Simple security attributes (authenticated policy)	FDP_IFC.1(2) FMT_MSA.3	Y
FDP_IFF.1(3)	Simple security attributes (export policy)	FDP_IFC.1(3) FMT_MSA.3	Y
FIA_AFL.1(1)	Authentication failure handling (console)	FIA_UAU.1	Y, see FIA_UAU.2
FIA_AFL.1(2)	Authentication failure handling (exponential backoff)	FIA_UAU.1	Y, see FIA_UAU.2

SFR Identifier	Name	Dependency	Dependency Met
FIA_SOS.1	Verification of Secrets	NONE	Y
FIA_UAU.2	User authentication before any action	FIA_UID.1	Y, see FIA_UID.2
FIA_UID.2	User identification before any action	NONE	Y
FIA_UAU.5	Multiple authentication mechanisms	NONE	Y
FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1 FMT_SMF.1	Y
FMT_MSA.1	Management of security attributes	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Y
FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	Y
FMT_SMF.1	Specification of management functions	NONE	NA
FMT_SMR.1	Security roles	FIA_UID.1	Y, see FIA_UID.2
FPT_ITA.1	Inter-TSF availability within a defined availability metric	NONE	Y
EXT_FPT_ITA(1)	Inter-TSF availability with a defined availability metric (RADIUS/TACACS+)	NONE	Y
EXT_FPT_ITA(2)	Inter-TSF availability with a defined availability metric (NTP)		
FTA_SSL.3	TSF-initiated termination,	NONE	NA
FTA_SSL.4	User-initiated termination	NONE	NA
FTA_TSE.1	TOE session establishment (Remote)	NONE	NA

Table 6 - Security Functional Requirement Dependencies

8.2.3.2 Justification for Unsatisfied Dependencies

There are no unsatisfied dependencies.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE Security Functions Rationale

Table 7 provides a bi-directional mapping of Security Functions to Security Functional Requirements. It shows that each of the SFRs is addressed by at least one of the Security Functions and that each of the Security Functions addresses at least one of the SFRs. For a description of how each Security Functional Requirement is addressed by the corresponding Security Function refer to section 7, TOE Summary Specification.

	F.AUDIT	F.I&A	F.SECURITY MANAGEMENT	F.TOE ACCESS	F.USER DATA PROTECTION	F.TSF_PROTECTION	F.CONSOLE_ACCESS
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FDP_ETC.2					X		
FDP_IFC.1(1)					X		
FDP_IFC.1(2)					X		X
FDP_IFC.1(3)					X		
FDP_IFF.1(1)					X		
FDP_IFF.1(2)					X		X
FDP_IFF.1(3)					X		

	F.AUDIT	F.I&A	F.SECURITY MANAGEMENT	F.TOE ACCESS	F.USER DATA PROTECTION	F.TSF_PROTECTION	F.CONSOLE_ACCESS
FIA_AFL.1(1)		X					
FIA_AFL.1(2)		X					
FIA_SOS.1		X					
FIA_UAU.2		X					
FIA_UID.2		X					
FIA_UAU.5		X					
FMT_MOF.1			X				X
FMT_MSA.1			X				X
FMT_MSA.3			X				X
FMT_SMF.1			X				X
FMT_SMR.1			X				X
FPT_ITA.1						X	
EXT_FPT_ITA.1(1)						X	
EXT_FPT_ITA.1(2)						X	
FTA_SSL.3				X			
FTA_SSL.4				X			
FTA_TSE.1				X			

Table 7 - Mapping of Security Functions to Security Functional Requirements