SECURITY TARGET

FOR

ALCATEL-LUCENT 7-SERIES SERVICE ROUTER OPERATING SYSTEM (SROS) FAMILY

Evaluated Assurance Level: 3+

Document No. 1868-001-D001

Version: 0.14, 16 June 2015

Prepared for:

Alcatel-Lucent

701 East Middlefield Road

Mountain View, CA

USA, 9403

Prepared by:

Electronic Warfare Associates-Canada, Ltd.

1223 Michael St., Suite 200

Ottawa, Ontario

K1J 7T2

and

Saffire Systems

PO Box 40295

Indianapolis, IN 46240

AMENDMENT RECORD SHEET

Rev.	Issue Date	Description	Author	Reviewer
0.1	1 March 2014	Initial edits by Alcatel-Lucent review	C. Rajsic	Greg Lague
0.2	15 April 2014	Initial draft for Alcatel-Lucent review	M. Ruppel, Saffire Systems	Carl Rajsic
0.3	16 April 2014	Updates from Alcatel-Lucent review	M. Ruppel, Saffire Systems	Bruce Gordon
0.4	28 April 2014	Updates from EWA review	M. Ruppel, Saffire Systems	Bruce Gordon
0.5	01 May 2014	Updates from EWA review	M. Ruppel, Saffire Systems	Bruce Gordon
0.6	06 May 2014	Add documentation titles for 7705 & 7210 platforms	M. Ruppel, Saffire Systems	Bruce Gordon
0.7	07 July 2014	Updates from EWA CEM review	M. Ruppel, Saffire Systems	Bruce Gordon
0.8	19 August 2014	Address comments from Combitech	M. Ruppel, Saffire Systems	Anders Staaf
0.9	10 December 2014	Changed 7210 SAS version/build number. Removed FDP_ETC.2, and *_ITA requirements.	M. Ruppel, Saffire Systems	
0.10	10 December 2014	Correcting OS names and terminology.	M. Ruppel, Saffire Systems	
0.11	22 December 2014	Updated documentation list and added non-evaluated feature list. Changed to SAS v7.0. Removed availability claims.	M. Ruppel, Saffire Systems	
0.12	18 March 2015	Added features to the Non-evaluated Funciton/Features list.	M. Ruppel, Saffire Systems	
0.13	23 March 2015	Reorganized the Non-evaluated features section.	M. Ruppel, Saffire Systems	
0.14	16 June 2015	Updated CPM filter/queue description and documentation list. Disallowed use of FTP. Updated FAU_GEN.1, FIA_SOS.1, and FDP_IFF.1(1) SFRs.	M. Ruppel, Saffire Systems	

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the *Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family*, hereafter referred to generically as *SROS*, 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 *SROS* satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

This document is structured as follows:

- Section 1 - Introduction provides the ST reference, the TOE reference, the TOE overview and the TOE description.
- Section 2 - Conformance Claims describes how this ST conforms to the Common Criteria and Packages. This ST does not conform to a Protection Profile.
- Section 3 - Security Problem Definition describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.
- Section 4 - Security Objectives defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition
- Section 5 - Extended Components Definition defines the extended components which are then detailed in Section 6.
- Section 6 - Security Requirements specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.
- Section 7 - TOE Summary Specification describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.
- Section 8 - Other References identifies reference documents beyond the TOE guidance documentation listed in Section 1.6.11 that are either referred to directly in this Security Target or aid in better understanding the TOE and the application of its technology.

1.2 SECURITY TARGET REFERENCE

This Security Target is uniquely identified as depicted in Table 1.

Table 1: Security Target Reference

Title	Security Target for the Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family
Version Number	Version 0.14
Publication Date	10 July 2015
Author	Electronic Warfare Associates – Canada Ltd. (EWA-Canada) Saffire Systems

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation (TOE) for this Security Target (ST) is the *Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family* (*SROS*) consisting of the following:

a. *Alcatel-Lucent 7x50 Service Router Operating System (SR OS), v12.0*. The specific build number is 12.0R4.

b. *Alcatel-Lucent 7705 Service Aggregation Router Operating System (SAR OS), v6.1*. The specific build number is 6.1R4.

c. *Alcatel-Lucent 7210 Service Access Switch Operating System (SAS OS), v7.0* .The specific build number is 7.0R1.

The *SROS* runs on the router and switch platforms and models listed in Table 2. The hardware for the models listed in Table 2 is excluded from the TOE boundary with the exception of:

a. CPM hardware queues for the XRS, SR, ESS and SAS models, which are included in the TOE boundary; and

b. CSM hardware queues for the SAR models, which are included in the TOE boundary.

Table 2: Platforms Supported by SROS

Platform	Model(s)	Hardware Queue	Models with CPU Protection	Operating System	Collective Reference Terms
7950 Extensible Routing System (XRS)	XRS-40, XRS-20, XRS-16c	CPM	XRS-40, XRS-20, XRS-16c	*SR OS v12.0*	7x50 or XRS/SR/ESS
7750 Service Router (SR)	SR-12e, SR-12, SR-7, SR-c12, and SR-c4	CPM	SR-7, SR-12		
7450 Ethernet Services Switch (ESS)	ESS-1, ESS-6, ESS-6v, ESS-7, and ESS-12	CPM	ESS-6, ESS-7, ESS-12		
7705 Service Aggregation Router (SAR)	SAR-18, SAR-8, SAR-F, SAR-M, SAR-W, SAR-Wx, SAR-H, and SAR-Hc.	CSM		*SAR OS v6.1*	7705 or SAR
7210 Service Access Switch (SAS)	SAS-D, SAS-E, SAS-M, SAS-M (10GIGE), SAS-X, SAS-T and SAS-R6	CPM		*SAS OS v7.0*	7210 or SAS

1.4 TERMINOLOGY AND ACRONYMS

The following terms and acronyms as used within this Security Target have the meanings defined herein.

1.4.1 Terminology

The following terminology is used in this ST:

7210	A collective term used in this document to refer to Alcatel-Lucent 7210 SAS service access switches. Refer to Table 2 for additional information.
7705	A collective term used in this document to refer to Alcatel-Lucent 7705 SAR service aggregation routers. Refer to Table 2 for additional information.
7x50	A collective term used in this document to refer to Alcatel-Lucent 7950 XRS extensible routing systems, 7750 SR and SRc service routers as well as 7450 ESS Ethernet services switches. Refer to Table 2 for additional information.
Access Control List	An Access Control List (ACL) is filter policy applied on ingress or egress to a service SAP on an interface to control the traffic access.
Adapter Card	SAR-series routers and SAS-series switches employ Adapter Cards in which physical interfaces terminate. See also Media Dependent Adapter (MDA) for XRS/SR/ESS-series devices.
Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family	The Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family (SROS) is the Target of Evaluation (TOE). The SROS consists of the following software configuration items (CIs): a. Alcatel-Lucent 7x50 Service Router Operating System (SR OS), v12.0; b. Alcatel-Lucent 7705 Service Aggregation Router Operating System (SAR OS), v6.1; and c. Alcatel-Lucent 7210 Service Access Switch Operating System (SAS OS), v7.0. These software CIs operate on the routers and switches listed in Table 2.
Asynchronous Transfer Mode	Asynchronous Transfer Mode (ATM) is a standardized digital data transmission technology. ATM is a cell-based switching technique that uses asynchronous time division multiplexing.
Border Gateway 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 rule sets.
Central Processing Unit	All traffic destined to the CPM and CSM and that will be processed by its CPU
Command Line Interface	The Command Line Interface (CLI) is a terminal-based administrator interface used to configure a 7x50 XRS/SR/ESS, 7705 SAR, or 7210 SAS node.
Committed Information Rate	Committed Information Rate (CIR) is the amount of bandwidth that the carrier is committed to provide to the subscriber.

Control and Switching Module	The Control and Switching Module (CSM) is a module within the SAR devices. The CSM is functionally the same as the CPM on the XRS/SR/ESS/SAS-series devices.
Control Processor Module	The Control Processor Module (CPM) is a module with the XRS/SR/ESS and SAS-series devices. The CPM is functionally the same as the CSM on the SAR-series devices.
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.
Coordinated Universal Time	Coordinated Universal Time (UTC) is the definitive reference time scale. Time zones around the world may be expressed as positive or negative offsets from UTC. UTC is derived from International Atomic Time (TAI).
CPM Filter	XRS/SR/ESS routers and switches use separate CPM modules that 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. On the SAR-series of routers and switches CPM filter functionality is performed in Softtware and is know as CSM filter. CPM filters are not supported on the SAS-series.
CPU Protection	CPU protection protects the CPU of the node that it is configured on from a DoS attack by limiting the amount of traffic coming in from one of its ports and destined to the CPM (to be processed by its CPU) using a combination of the configurable limits. Some of the limits are configured globally for the node, and some of the limits are configured in CPU Protection profiles which are assigned to interfaces. CPU protection features are supported on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS-40/XRS-20/XRS-16c platforms.
CSM Filter	SAR-series routers with separate CSM modules (7705 SAR-M, SAR-8 and SAR-18 models) have traffic management and queuing hardware on the CSM modules dedicated to protecting the Control Plane. CSM filters are created on this hardware and instantiated by the operating system without user interference. 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. On 7705 SAR-8 and SAR-18 nodes, the CSM is a redundant and pluggable module. On 7705 SAR-F and SAR-M nodes, the CSM is non-redundant and not pluggable.
Customer Premise Equipment	Customer Premise Equipment (CPE) is equipment that is installed in customer premises by a service provider to connect to a specific service.
Documented Special Use Addresses	Documented Special Use Addresses (DUSA) use IPv4 addresses
Ethernet Service Switch	Ethernet Service Switch (ESS) refers to the 7450 ESS series routers.

Ethernet Services Switch	Ethernet Services Switch (ESS) is a collective term used in this document to refer to the four 7450 ESS switch models listed in Table 2.
Frame Relay	Frame Relay (FR) is 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.
Generic Routing Encapsulation	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.
Hardware Queue	The CPM and CSM implement hardware queues to guarantee fair and "non-blocking" access to shared CPU resources.
In-band	In-band (IB) refers to interfaces using a physical I/O port on the router.
Input Output Module	An Input Output Module (IOM) is router module that interconnects two Media Dependent Adapters (MDAs) or Adapter Cards with the fabric core. This module also performs Layer 3 traffic management. Part of Data Plane.
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.
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.
Internet Protocol	The Internet Protocol (IP) is 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.
Label Distribution Protocol	The Label Distribution Protocol (LDP) is a new protocol that defines a set of procedures and messages by which one LSR (Label Switch Router) informs another of the label bindings it has made.
Label Switch Path	A Label Switch Path (LSP) is a sequence of hops in which a packet travels by label switching.
Label Switch Router	A Label Switch Router (LSR) is a node capable of forwarding datagrams based on a label.
Link Aggregation Group	Link Aggregation Group (LAG) is 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.

Local Area Network	A Local Area Network (LAN) is a system designed to interconnect computing devices over a restricted geographical area (usually not more than a couple of kilometres).
Management Access Filter	A Management Access Filter (MAF) controls all traffic in and out of the CPM. A MAF can be used to restrict management of the XRS/SR/ESS-Series device by other nodes outside either specific (sub)networks or through designated ports. For SAR and SAS-series devices, MAFs also control all traffic in and out of the CSM/CPM. They can be used to restrict management of the SAR or SAS by other nodes outside specific (sub)networks or through designated ports.
Management Information Base	A Management Information Base (MIB) is a type of database used for managing the devices in a communications network.
Maximum Burst Size	Maximum Burst Size (MBS) is one of the parameters associated with queue configuration in the TOE. This is the maximum buffer space available for the traffic flows associated with the queue.
Media Access Control	Media Access Control (MAC) is a media-specific access control protocol within IEEE 802 specifications. The protocol is for medium sharing, packet formatting, addressing, and error detection.
Media Dependent Adapter	A Media Dependent Adapter (MDA) is a module in XRS/SR/ESS-Series routers and switches that is housed in an IOM and in which a physical interface terminates. See also Adapter Cards for SAR and SAS-series devices.
Multicast Source Discovery Protocol	Multicast Source Discovery Protocol (MSDP) is a computer network protocol in the Protocol Independent Multicast (PIM) family of multicast routing protocols.
Multi-Protocol Label Switching	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.
Open Shortest Path First	Open Shortest Path First (OSPF) is a link-state routing algorithm that is used to calculate routes based on the number of routers, transmission speed, delays and route cost.
Out-of-band	Out-of-band (OOB) to the RS-232 Console port or the management Ethernet port on the SR.
Quality of Service	Quality of Service (QoS) is a set of performance parameters that characterize the traffic over a given connection
Remote Authentication Dial-In User Service	Remote Authentication Dial-In User Service (RADIUS) is 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.
Request for Comments	A Request for Comments (RFC) is an Internet Engineering Task Force (IETF) memorandum on Internet systems and standards
Route Table Manager	The Route Table Manager (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.

Routing Information Protocol	The 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.
RS-232	RS-232 is a serial communications protocol currently defined by **[TIA-232-F]**
SAR	SAR is a collective term used in this document to refer to the 7705 SAR-series routers using the SAR OS v6.1 operating system.
SAS	SAS is a collective term used in this document to refer to the 7210 SAS-series switches using the SAR OS v7.0 operating system.
Service Access Point	A Service Access Point (SAP) identifies the customer interface point for a service on a XRS/SR/ESS, SAR, or SAS.
Service Access Switch	Service Access Switch (SAS) is a collective term used in this document to refer to the five 7210 SAS switch models listed in Table 2.
Service Aggregation Router	Service Aggregation Router (SAR) is a collective term used in this document to refer to the four 7705 SAR router models listed in Table 2.
Service Aware Manager	The Service Aware Manager (SAM) provides GUI management functions (e.g., provisioning) for the XRS/SR/ESS, SAR, and SAS-series platforms. The SAM is defined outside the TOE boundary with a Console CLI (provides administrators with backside services) also outside the TOE boundary. All of the routers and switches listed in Table 2 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
Service Router	Service Router (SR) is a collective term used in this document to refer to the three 7750 SR router models and two 7750 SRc router models listed in Table 2.
XRS/SR/ESS	XRS/SR/ESS is a collective term used in this document to refer to the 7x50 series of SR routers and ESS switches listed in Table 2.
SRc	SRc is a collective term used in this document to refer to Alcatel-Lucent 7750 SRc service routers. Refer to Table 2 for additional information.
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).

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).
Terminal Access Controller Access Control System Plus	Terminal Access Controller Access Control System Plus (TACACS+) is 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.
Time to Live	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.
Transmission Control Protocol	The 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.
User Datagram Protocol	The User Datagram Protocol (UDP) is a is transport layer protocol which do not guarantee delivery of data.
Virtual Private Network	A Virtual Private Network (VPN) is a way to provide secure and dedicated communications between a group of private servers over public Internet.
VPN Routing and Forwarding	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.

1.4.2 Acronyms

The following acronyms are used in this ST:

ACL	Access Control List
ADV	Assurance Development (Common Criteria)
AGD	Assurance Guidance Documents (Common Criteria)
ALC	Assurance Life Cycle (Common Criteria)
ANSI	American National Standards Institute
AS	Autonomous System(s)
ASE	Assurance Security Target Evaluation (Common Criteria)
ATE	Assurance Tests (Common Criteria)
ATM	Asynchronous Transfer Mode
AVA	Assurance Vulnerability Assessment (Common Criteria)
BGP	Border Gateway Protocol
CB	Certification Body (Common Criteria)
CC	Common Criteria for Information Technology Security Evaluation (Common Criteria)
CCEF	Common Criteria Evaluation Facility (Common Criteria)
CCS	Canadian Common Criteria Evaluation and Certification Scheme (Common Criteria)

CEM	Common Evaluation Methodology (Common Criteria)
cf	Compact Flash
CIR	Committed Information Rate
CLI	Command Line Interface
CMA	Compact Media Adapter
CPE	Customer Premise Equipment
CPM	Control Processor Module
CPMQ	Control Processor Module Queuing
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSM	Control and Switching Module
D/DoS	Distributed Denial of Service
DES	Description (Common Criteria)
DoS	Denial of Service
DUSA	Documented Special Use Addresses
EAL	Evaluation Assurance Level (Common Criteria)
EAL 3+	Evaluation Assurance Level 3, Augmented (Common Criteria)
eBGP	External Border Gateway Protocol
ESS	Ethernet Service Switch Refer to the 7450 ESS-series of switches listed in Table 2
FC	Forwarding Class
FR	Frame Relay
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
I&A	Identification and Authentication
I/O	Input / Output
IB	In-band
iBGP	Internal Border Gateway Protocol
ID	Identification (or Identity)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IOM	Input Output Module
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
ISP	Internet Services Provider
IT	Information Technology
LACP	Link Aggregation Control Protocol (Ethernet LAG Control)
LAG	Link Aggregation Group
LAN	Local Area Network
LDP	Label Distribution Protocol

LED	Light Emitting Diode
LMI	Local Management Interface (e.g., ATM, Ethernet and Frame Relay)
LSP	Label Switch Path
LSR	Label Switch Router
MAC	Media Access Control
MAF	Management Access Filter
MBS	Maximum Burst Size
MDA	Media Dependent Adapter
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MSDP	Multicast Source Discovery Protocol
NTP	Network Time Protocol
OAM	Operation, Administration, and Maintenance
OBJ	Security Objectives (Common Criteria)
OE	Operational Environment
OOB	Out-of-band
OSP	Organizational Security Policies (Common Criteria)
OSPF	Open Shortest Path First
PCB	Printed Circuit Board
PDH	Plesiochronous Digital Hierarchy
PIM	Protocol Independent Multicast
PIM	Protocol Independent Multicast
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
REQ	IT Security Requirements (Common Criteria)
RFC	Request for Comments
RIP	Routing Information Protocol
RS-232	Serial protocol
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RTM	Route Table Manager
SAM	Service Aware Manager
SAM-A	SAM Assurance (module)
SAM-E	SAM Element Manager (module)
SAM-P	SAM Provisioning (module)
SAP	Service Access Point
SAR	Security Assurance Requirement
SAR	Service Aggregation Router
	See the family of 7705 SAR routers listed in Table 2.
SAS	Service Access Switch
	See the family of 7210 SAS switches listed in Table 2.
SCP	Secure Copy
SDH	Synchronous Digital Hierarchy
SDP	Service Distribution Point
SFP	Security Function Policy (Common Criteria)
SFR	Security Functional Requirement

SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SR	Service Router Refer to the 7750 SR and 7750 SRc family of routers listed in Table 2
SROS	Service Router Operating System Refer to the definition of "*Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family*" on page 8 for more information.
SSH	Secure Shell (protocol)
ST	Security Target (Common Criteria)
TACACS+	Terminal Access Controller Access Control System Plus
TAI	International Atomic Time
tar	File format used for archiving data (derived from "tape archive")
TCP	Transmission Control Protocol
TCP/IP	Transport Control Protocol over Internet Protocol
TOE	Target of Evaluation
TOE	Target of Evaluation (Common Criteria)
TSF	TOE Security Functionality (Common Criteria)
TSFI	TOE Security Functionality Interface (Common Criteria)
TSS	TOE Summary Specification (Common Criteria)
TTL	Time to Live
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VRF	VPN Routing and Forwarding
W3C	World Wide Web Consortium
XML	Extensible Mark-up Language
XRS	Extensible Routing System
XRS/SR/ESS	Extensible Routing / System Service Router / Ethernet Service Switch / Refer to the 7x50 family listed in Table 2

1.5 TOE OVERVIEW

1.5.1 TOE Type

The TOE is an Extensible Routing System (XRS) / Service Router (SR) / Ethernet Service Switch (ESS) / Service Aggregation Router (SAR) / Service Access Switch (SAS).

Alcatel-Lucent 7950 Extensible Routing Systems (XRSs) are deployed in service provider environments, 7750 Service Routers (SRs) are deployed in a multi-service edge routing environment, and the 7450 Ethernet Service Switches (ESSs) are deployed in a Metro Ethernet/MPLS aggregation environment.

7705 Service Aggregation Routers (SARs) and 7210 Service Access Switches (SASs) are typically deployed in mobile backhaul networks, fixed backhaul networks, and strategic industries' networks (including power infrastructure companies, train operations, emergency services, government, etc.).

1.5.2 Usage

The Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family (SROS) is designed to provide the functionality for infrastructure class telecom equipment including the Alcatel-Lucent 7950 Extensible Routing System (XRS), 7750 Service Routers (SRs), 7450 Ethernet Service Switches (ESSs), 7705 Service Aggregation Routers (SARs), and 7210 Service Access Switches (SASs). Internet Protocol (IP) and Multi-Protocol Label Switching (MPLS) networks based on the Alcatel-Lucent 7750 SR / SRc family 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 7950 XRS family of routers is deployed in service provider environments and is designed for scalability, efficiency and versatility.

The 7950 XRS, 7750 SR/SRc, 7450 ESS, 7705 SAR, and 7210 SAS devices 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), Plesiochronous Digital Hierarchy (PDH), Ethernet, Synchronous Optical Networking (SONET), Optical Transport Hierarchy (OTH), and serial and analog interfaces. Forwarding Technology employed in the product includes Layer 2/Layer 3 encapsulation and Internet Protocol (IP), MPLS/ Media Access Control (MAC) forwarding lookup.

The 7750 SR/SRc offers service providers and enterprises differentiated services 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 7705 SAR and 7210 SAS nodes provide service providers with the means to aggregate service delivery in fixed and mobile backhaul networks. The 7950 XRS offers service provides the ability to meet all IP core routing, MPLS switching, data center interconnection and VLL/VPN infrastructure service needs in metro cores and IP backbones.

The Alcatel-Lucent 7-SROS family offer the ability to configure an SSH server to establish secure connection to/from the SROS. It also supports network access control of client devices on an Ethernet network using the IEEE 802.1x standard. The Alcatel-Lucent 7-SROS family also offers the ability to manage the devices using Simple Network Management Protocol (SNMP).

1.5.3 Security Features

The major security features of the Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family 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 SROS also provides protection against the Denial of Service (DoS) attacks.

1.5.4 TOE Operational Environment

1.5.4.1 General

The XRS/SR/ESS, SAR and SAS all have the ability to monitor, route, and manipulate network traffic to facilitate its delivery to the proper destination on a network or between networks. The XRS/SR/ESS is typically 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 XRS/SR/ESS and the actual customer. There is typically a residential gateway in between the XRS/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 XRS/SR/ESS, SAR, or SAS and the customer network.

The SR can also be deployed in core network architectures, where the interconnection between different operator core networks is maintained. The interconnection between the different core routers relies on a different setup of operational protocols and aspects, compared to an SR deployment in an aggregation or residential network.

The SAR and SAS are primarily used in mobile backhaul networks as well as fixed backhaul and strategic industries (power infrastructure companies, train operations, emergency services, government, etc.). While it can be used to for residential services (via the SAR-18 platform), the scale of the XRS/SR/ESS is more suited for this situation.

For the XRS/SR/ESS, SAR or SAS to function, they must have physical access to at least two distinct networks or network segments to pass data between. These are devices that forward data packets along networks. The XRS/SR/ESS, SAR or SAS is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.

Between XRS/SR/ESSs/SARs/SASs, 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. To ensure proper operation of the network itself, the network elements can also communicate Operations, Management and Alarm (OAM) information via designated control channels to provide automatic monitoring of the data bearers, and take consecutive actions in the event of deviation from a pre-defined operational steady-state condition.

1.5.4.2 Physical Installation, Deployed Configuration and Interfaces

All TOE interfaces shown in,Figure 1with 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 operating system (i.e., SR OS v12.0, SAR OS v6.1, or SAS OS v7.0) located on a compact flash card. These operating systems run on the various hardware platforms listed in Table 2.

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 XRS/SR/ESS, SAS, or SAR. Each administrator can only be provided enough access to perform their duties on the network and no more.

The deployed configuration of the TOE uses filters and Access Control Lists (ACLs) to protect against Distributed and other DoS (D/DoS) attacks.

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

1.5.5 Hardware and Software Supplied by the IT Environment

This section identifies any non-TOE hardware, software, and firmware that is required by the TOE to operate correctly as specified herein.

The TOE is a software (and Control Processor Module (CPM) or Control and Switching Module (CSM)[1] hardware) TOE consisting of the Alcatel-Lucent 7-Series Service Router Operating System (SROS) Familywhich is an integral component of the Alcatel-Lucent service router product platforms and modules identified in Table 2.

The hardware for the models listed in Table 2 is excluded from the TOE boundary with the exception of:

- CPM hardware queues for the XRS, SR, ESS and SAS models, which are included in the TOE boundary; and
- CSM hardware queues for the SAR models, which are included in the TOE boundary.

For the 7x50 XRS/SR/ESS and 7210 SAS-series of devices, administrators allocate dedicated CPM hardware queues, as applicable, for certain traffic designated to the CPUs and set the corresponding rate-limit for the queues.

For the 7705 SAR, CSM queues are preset and tuned to prevent malicious attacks so no configuration is required by the Administrator. CSM filters on the 7705 SAR are configurable by the administrator.

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 behaviours, and the way they configured are the same in the 7x50 XRS/SR/ESS, 7705 SAR, and 7210 SAS routers and switches.

There is also the 5620 Service Aware Manager (SAM) which provides GUI management functions (e.g., provisioning) for 7x50 XRS/SR/ESS, 7705 SAR, and 7210 SAS devices. The 5620 SAM is defined outside the TOE boundary. Additionally, the Console Command Line Interface (CLI) (which provides administrators with backside services) is defined to be outside the TOE boundary. 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:

- 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+;
- SAM: SUN Solaris 10 or any 32-bit Windows operating system;
- SCP/remote CLI: Any combined hardware and operating system platform that supports the operation of the Secure Shell protocol;
- 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;

[1] The 7x50 XRS/SR/ESS and 7210 SAS platforms use CPMs whilst the 7705 SAR routers employ CSMs. These two modules have the same function but simply use a different nomenclature.

- Local Console/CLI: Any combined hardware and operating system platform that supports terminal emulation to the ANSI X3.64 standard; and
- NTP server: Any combined hardware and operating system platform that supports RFC 1305 for Network Time Protocol.

1.6 TOE DESCRIPTION

1.6.1 General

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

a. Management Plane subsystem;

b. Control Plane subsystem; and

c. Data Plane subsystem.

The SROS software uses a base real-time operating system (OS). The primary copy of SROS software is located on a compact flash card installed in the hardware platforms. The removable media is shipped with each model and contains a copy of the applicable SROS image (i.e., SR OS v12.0, SAR OS v6.1, or SAS OS v7.0).

1.6.2 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.

1.6.2.1 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 XRS/SR/ESS platforms by other nodes outside either specific (sub) networks or through designated ports.

MAFs allow the administrator to configure the following:

a. Destination UDP/TCP port number;

b. IP protocol ID;

c. Source port; and

d. 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.

1.6.2.2 Login Control Parameters

Login control parameters (for Console, Remote management[2]) 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.

1.6.2.3 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.

1.6.2.4 Authentication / Authorization

Access permission to the system are controlled:

a. remotely using either:

   (1) TACACS+; or

   (2) RADIUS; or

b. local to the network 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.

1.6.2.5 CPU Protection

The CPU protection feature, available on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms is designed to provide DoS protection by rate limiting control protocol traffic destined toward the CPM of the node.

1.6.2.6 Local Console Access

Local authentication[3] uses administrator names and passwords to authenticate login attempts.

1.6.3 Control Plane Subsystem

The Control Plane handles the dynamic protocols for the exchange of (reachability, topological, and resource state) information, allowing for an accurate forwarding operation. It provides other planes with pertinent information 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.

[2] 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.

[3] 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.

CPM/CSM filters control all traffic destined for the CPM/CSM, including all routing and OAM protocols. They apply to packets from all network and access ports, but not to packets from a management Ethernet port. CPM/CSM 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/CSM of a XRS/SR/ESS, SAS or SAR. The Switch Fabric (SF) / Control Processor Module (CPM) (or the Control and Switching Module (CSM) on SAR-series devices) controls the switching and routing and functions of the TOE.

The XRS/SR/ESS, SAS, and SAR provide CPM/CSM protection against the DoS attacks via the access control and quality of service mechanisms.

On the XRS/SR/ESS and SAR-series routers and switches filters can be installed for ingress management traffic destined either for the CPM/CSM Ethernet port or any other logical port (LAG, port, or channel) on the device to be subject of the filter-action. On the SAS-series, specific filters are installed to identify and direct control traffic to the CPU.

MAC/IP CPM/CSM filters and queues control all traffic going into the CPM/CSM, 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/CSM filters or IP CPM/CSM filters are used to perform a match and apply action using filter criteria.

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

The Control Plane on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12,and 7950 XRS platforms also includes the CPU protection feature which is designed to rate limit control protocol traffic destined towards the CPM of the node.The Route Table Manager (RTM) is a library with its own dedicated memory manager. RTM modification APIs are invoked from Routing Protocols or via static routing configuration. Routing and signalling protocols implemented are:

a. OSPFv2;

b. IS-IS;

c. BGP-4; and

d. MPLS (LDP, RSVP-TE).

1.6.4 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 SROS 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 “through” DoS and CPM queues used for the “to”.

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:

a. ip-filters; and

b. 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:

a. protocol related packets;

b. OAM packets; and

c. error indicating packets.

1.6.5 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 based on SSH or telnet 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.

1.6.6 In-Band Management Interface

In-band Management Interface involves management sessions to one of the SROS IP interfaces using a physical I/O (access or network) port on the device.

1.6.7 Secure Copy Protocol (SCP)

The administrator copies and manages software images, configuration files and log files via SCP[4]. All of these functions are performed through in-band interfaces and the OOB management Ethernet port.

1.6.8 Physical Scope

Figure 1 shows the TOE in its deployment configuration.

[4] Secure Copy Protocol (SCP) is a capability of the SR OS versions in the TOE; 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.

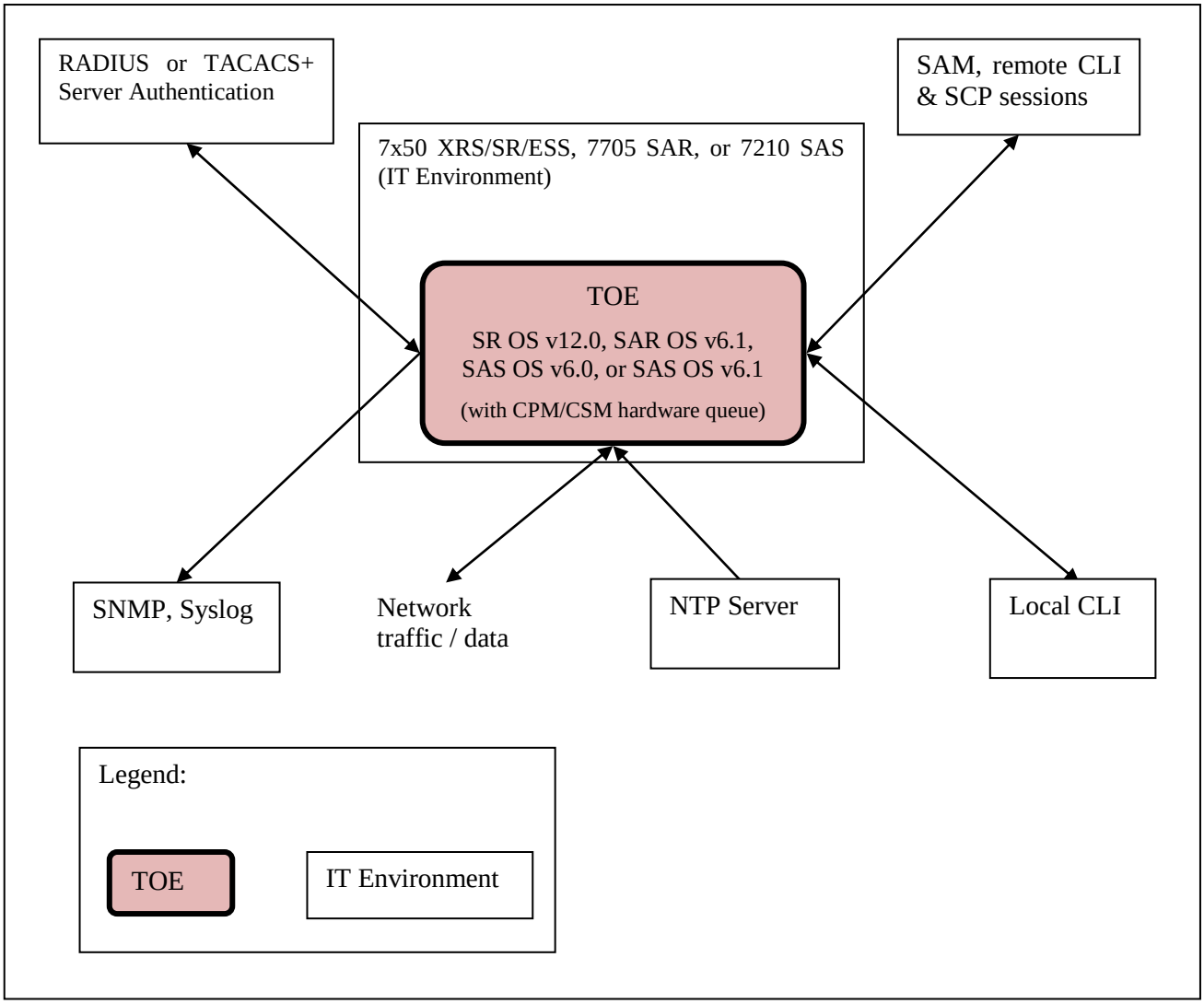

Figure 1: TOE Boundary

Note to Figure 1 *The physical boundary is the SROS operating system (i.e., SR OS v12.0, SAR OS v6.1, or SAS OS v7.0) located on a compact flash card. The SROS runs on various hardware platforms but the hardware platforms are excluded with the exception of the CPM/CSM hardware queues. The SROS assigns CPM/CSM hardware queues for certain traffic designated to the CPUs and set the corresponding rate-limit for the queues. These CPM/CSM 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.*

1.6.9 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 security relevant features described in the following subsections.

1.6.9.1 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.

1.6.9.2 Identification & Authentication (I&A)

SROS identifies and authenticates individual users by validating an administrator's username and password. Administrators are identified and authenticated via local authentication, RADIUS, or TACACS+. SROS also provides authentication failure handling and the ability for the administrator to define password complexity requirements.

1.6.9.3 Security Management

SROS implements authorization features, which allow the administrator to access and execute commands at various command levels based on profiles assigned to the administrator. The Administrator configures system security and access functions and logging features using CLI syntax and command usage to configure parameters.

1.6.9.4 TOE Access

Mechanisms place controls on Administrators' 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.

1.6.9.5 User data protection (Information flow control)

The SROS 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 SROS 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 SROS enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap, Syslog, and RADIUS/TACACS+ destinations.

1.6.9.6 TSF Protection

The SROS on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12,and 7950 XRS platforms includes the CPU protection feature which is designed to rate limit control protocol traffic destined towards the CPM of the node. The CPU protection feature can mitigate any type of DOS attack against these nodes. In addition, the CPU protection feature prohibits any protocol/software failure from adjacent nodes that start to generate control traffic above its expected rate from overwhelming the node and rate limits it within specs of the protocol.

This type of protection is critical at hub site or central locations where the size of nodes is processing very large amounts of data from many branch/remote locations at the central location. Typically these nodes are in data centers providing critical communications functions to servers and applications and must maintain operation at all times. Any downtime experienced by these nodes can have significant impact to operations and as such the CPU protection feature helps ensure that these nodes remain operational if attacked, or protocol/software failures occur that may jeopardize normal node functions. The larger ALU 7950/7750/7450

nodes (specifically the SR-7/SR-12, ESS-6/ESS-7/ESS-12 and 7950 XRS) are used in these centralized functions and provide the added CPU protections needed. The other ALU nodes are typically found at branch and remote locations where this added CPU protection capability is not as critical for normal network function, and therefore is not included in those series of nodes.

1.6.9.7 Local/remote Console Access

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

1.6.10 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 SROS (CLIENT-side) for:

   (1) RADIUS or TACACS+ server authentication/ authorization services;

   (2) local Console access for most administration;

   (3) SNMP/Syslog servers for logging; and

   (4) Network Time Protocol (NTP) server for external time synchronization;

b. Enable Routing protocols from this set:

   (1) OSPFv2;

   (2) IS-IS;

   (3) BGP-4; and

   (4) MPLS (LDP, RSVP-TE);

c. Ensure Telnet and FTP remain disabled;

d. Use SNMPv3 only;

e. Configure MAF filters on the XRS/SR/ESS, SAR, and SAS devices to restrict access to management ports on the device;

f. Configure CPM/CSM filters on XRS/SR/ESS, and SAR devices for DoS attack protection against router appliance and network;

g. Configure CPM Queues on XRS/SR/ESS for bandwidth restrictions as a protection against DoS attacks targeting the network;

Application Note: *7705 SAR CSM Queues and 7210 SAS CPM filters and queues are not configurable. These mechanisms are fixed in terms of usage (i.e., each queue handles a specific type of traffic) and configuration (i.e., each queue is configured for specific rates and buffering capacities). To avoid DoS-like attacks overwhelming the Control Plane, while ensuring that critical control traffic (such as signalling) is always serviced in a timely manner, the 7705 SAR has three queues (High, Low, and Ftp) for handling packets addressed to the CSM:*

High: handles all messaging which is important for keeping the network stable from a control plan point of view. The messages in this queue are related to network management, signalling, routing, etc.

Low: handles messages that can be treated with a lower importance when doing so has no detrimental impact on the overall stability of the network. Examples include ICMP ECHO REQ (pings), etc.

Ftp: handles messages related to bulk file transfers. These types of messages require appropriate buffering with little or no CSM interference. Examples include the ftp download of a new software image, etc.

Application Note: Packets that are destined to the 7210 SAS CPU are prioritized based on the application. These include Layer 2 data packets (a copy of which is sent to CPU for MAC learning), EFM, CFM, STP, LACP, ICMP, etc. The CPU provides eight queues from BE (0) to NC (7). Packets destined to the CPU are classified internally and are put into the correct queue. These packets are rate-limited to prevent DoS attacks. The software programs the classification entries to identify these packets and assigns appropriate bandwidth and priority to them. As noted above, 7210 SAS CPM filters are not configurable by the user.

h. Configure Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) Time to Live (TTL) Security on XRS/SR/ESS;

Application Note: BGP is not included in the scope for SAR or SAS for this Evaluation. These devices can support BGP as part of a VPRN (label distribution) and as an exterior protocol for VPRN (eBGP). But the 7705 SAR and the 7210 SAS do not provide typical boarder gateway functions such as RR, iBGP, eBGP for traditional ISP type boundaries.

i. Enforce/enable/configure a strong password policy;

j. 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; and

k. Configure CPU Protection on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms to rate limit control traffic destined to the CPM.

l. Use SSHv2 only (SSHv1 is not allowed)

1.6.11 Non-evaluated Functions/Features

This section identifies the features of the SROS product family that are outside from the evaluated configuration.

The following features of the SROS product family are outside the evaluated configuration. Their use is allowed in the evaluated configuration, but the features have not been tested.

1. The 7750 SR/SRc offers service providers and enterprises differentiated services, from Internet access to multipoint Virtual Private Network (VPN) over a single network infrastructure. VPN is a capability of the SR OS; however, it is defined outside the TOE and was not evaluated.
2. High availability is an important feature in service provider routing systems. Downtime can be very costly, and, in addition to lost revenue, customer information and business-critical communications can be lost. High availability is the combination of continuous uptime over long periods (Mean Time Between Failures (MTBF)) and the speed at which failover or recovery occurs (Mean Time To Repair (MTTR). Network and service availability are critical aspects when offering advanced IP services which dictates that IP routers that are used to construct the foundations of these networks be resilient to component and software outages. The high availability feature is not in the scope of the evaluated configuration.

3. SSH/SCP secure communications is a capability of the SR OS; however, the underlining cryptographic protocols and associated cryptographic functionality are defined outside the TOE and part of the TOE's operational environment and not evaluated.
4. Border Gateway Protocol (BGP) is not in the scope of the evaluated configuration.

The following features of the SROS product family are not allowed in the evaluated configuration.

1. The use of Telnet and FTP is not allowed in the evaluated configuration.
2. The use of the Netconf server is not allowed in the evaluated configuration.
3. The use SNMPv1 and SNMPv2 are not allowed in the evaluated configuration.
4. The use of SSHv1 is not allowed in the evaluated configuration.
5. SROS is able to function as an NTP server; however that capability is excluded from the evaluated configuration. The use of NTP/SNTP server mode is not allowed in the evaluated configuration, neither is multicast/broadcast mode.

1.7 TOE GUIDANCE DOCUMENTATION

The guidance documentation that accompanies the TOE is listed in the following subsections.

1.7.1 7x50 XRS/SR/ESS (SR OS v12.0R4) Guidance Documentation

[93-0400-03-02] *7950 SR-OS Basic System Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0400-03-02 Edition 1, 2014

[93-0401-03-02] *7950 SR OS System Management Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0401-03-01 Edition 01, 2014

[93-0402-03-02] *7950 SR-OS Interfaces Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0402-03-02 Edition 01, 2014

[93-0403-03-02] *7950 SR-OS Router Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0403-03-02 Edition 1, 2014

[93-0404-03-02] *7950 SR OS Routing Protocols Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0404-03-02 Edition 1, 2014

[93-0405-03-02] *7950 SR OS MPLS Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0405-03-02 Edition 01, 2014

[93-0406-03-02] *7950 SR OS Services Guide*, Software Version: Service Router Release 12.0, Alcatel-Lucent Document Part Number: 93-0406-03-02 Edition 01, 2014

[93-0407-03-02] *7950 SR OS Quality of Service Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0407-03-02 Edition 1, 2014

[93-0408-03-02] *7950 SR-OS OAM and Diagnostics Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0408-03-02 Edition 01, 2014

[93-0070-11-02] *7750 SR-OS Basic System Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0070-11-02 Edition 1, 2014

[93-0071-11-02]	*7750 SR OS System Management Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0071-11-02 Edition 01, 2014
[93-0072-11-02]	*7750 SR-OS Interfaces Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0072-11-02 Edition 01, 2014
[93-0073-11-02]	*7750 SR-OS Router Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0073-11-02 Edition 1, 2014
[93-0074-11-02]	*7750 SR OS Routing Protocols Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0074-11-02 Edition 1, 2014
[93-0075-11-02]	*7750 SR OS MPLS Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0075-11-02 Edition 01, 2014
[93-0076-11-02]	*7750 SR OS Services Guide*, Software Version: Services Guide Release 12.0 Release 4, Alcatel-Lucent Document Part Number: 93-0076-11-02 Edition 01, 2014
[93-0077-11-02]	*7750 SR OS Quality of Service Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0077-11-02, Edition 01, 2014
[93-0098-10-02v2]	*7750 SR OS Triple Play Guide*, Software Version: Triple Play Service Delivery Architecture Guide Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0098-10-02v2, 2014
[93-0181-08-02]	*7750 SR-OS OAM and Diagnostics Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0181-08-02 Edition 01, 2014
[93-0099-11-02]	*7450 ESS OS Triple Play Guide*, Software Version: Service Aggregation Router OS Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0099-11-02 Edition 01, 2014
[93-0100-11-02]	*7450 ESS-OS Basic System Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0100-11-02 Edition 1, 2014
[93-0101-11-02]	*7450 ESS OS System Management Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0101-11-02 Edition 01, 2014
[93-0102-011-02]	*7450 ESS OS Interfaces Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0102-011-02 Edition 01, 2014
[93-0103-11-02]	*7450 ESS-OS Router Configuration Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0103-11-02 Edition 1, 2014
[93-0104-11-02]	*7450 ESS OS Routing Protocols Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0104-11-02 Edition 1, 2014
[93-0105-11-02]	*7450 ESS OS Quality of Service Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0105-11-02, Edition 1, 2014
[93-0106-11-02]	*7450 ESS OS MPLS Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0106-11-02 Edition 01, 2014

[93-0107-11-02]	*7740 ESS OS Services Guide*[5], Services Guide Release 12.0 Release 4, Alcatel-Lucent Document Part Number: 93-0107-11-01 Edition 01, 2014
[93-0183-08-02]	*7450 ESS-OS OS OAM and Diagnostics Guide*, Software Version: Service Router Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0183-08-02 Edition 01, 2014
[93-0262-05-02]	*OS Multi-Service Integrated Services Adapter Guide*, Software Version: MS-ISA Guide Release 12.0 R4, Alcatel-Lucent Document Part Number: 93-0262-05-02 Edition 02, 2014
[93-0267-04-01]	*Advanced Configuration Guide*, Software Version: Advanced Configuration Release 12.0 R1, Alcatel-Lucent Document Part Number: 93-0267-04-01, 2014

1.7.2 7705 SAR (SAR OS v6.1R4) Guidance Documentation

[3HE 08670 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 Basic System Configuration Guide*, Software Versions: Service Aggregation Router OS Release 6.1 R4, 2014, Part Number: 3HE 08670 AAAB TQZZA Edition 01
[3HE 08669 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 Interface Configuration Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08669 AAAC TQZZA Edition 01
[3HE 08672 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 MPLS Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08672 AAAC TQZZA Edition 01
[3HE 08671 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 OAM and Diagnostics Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08671 AAAC TQZZA Edition 01
[3HE 08673 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 Quality of Service Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08673 AAAC TQZZA Edition 01
[3HE 08674 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 Router Configuration Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08674 AAAC TQZZA Edition 01
[3HE 08675 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 Routing Protocols Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08675 AAAC TQZZA Edition 01
[3HE 08676 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 Services Guide*, Software Version: Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08676 AAAC TQZZA Edition 01
[3HE 08677 AAAC TQZZA Edition 01]	*Alcatel-Lucent 7705 System Management Guide*, Software Version Service Aggregation Router OS Release 6.1 R4, 2014, Document Part Number: 3HE 08677 AAAC TQZZA Edition 01

1.7.3 7210 SAS (SAS OS v7.0R1) Guidance Documentation

[3HE09520AAAA]	*Alcatel-Lucent 7210 SAS D, E OS Basic System Configuration Guide*, Software Versions: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09520AAAA

[5] This is really the 7450 ESS OS Services Guide as noted by the footers in the document and the preface.

[3HE09518AAAA] *Alcatel-Lucent 7210 SAS D, E OS Interface Configuration Guide*, Software Version: Service Access Switch Release 7.0 Rev .01, 2014, Document Part Number: 3HE09518AAAA

[3HE09526AAAA] *Alcatel-Lucent 7210 SAS D, E OS OAM and Diagnostics Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09526AAAA

[3HE09515AAAA] *Alcatel-Lucent 7210 SAS D, E OS Quality of Service Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09515AAAA

[3HE09528AAAA] *Alcatel-Lucent 7210 SAS D, E OS Router Configuration Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09528AAAA

[3HE09524AAAA] *Alcatel-Lucent 7210 SAS D, E OS Routing Protocols Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09524AAAA

[3HE09516AAAA] *Alcatel-Lucent 7210 SAS-M and 7210 SAS-T OS Quality of Service Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09516AAAA

[3HE09521AAAA] *Alcatel-Lucent 7210 SAS M, T, X, R6 OS Basic System Configuration Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09521AAAA

[3HE09519AAAA] *Alcatel-Lucent 7210 SAS M, T, X, R6 OS Interface Configuration Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09519AAAA

[3HE09527AAAA] *Alcatel-Lucent 7210 SAS M, T, X, R6 OAM and Diagnostics Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09527AAAA

[3HE09519AAAA] *Alcatel-Lucent 7210 SAS M, T, X, R6 OS Router Configuration Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01 2014 Document Part Number: 3HE09529AAAA

[3HE09525AAAA] *Alcatel-Lucent 7210 SAS M, T, X, R6 OS Routing Protocols Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09525AAAA

[3HE09517AAAA] *Alcatel-Lucent 7210 SAS-X and 7210 SAS-R6 OS Quality of Service Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09517AAAA

[3HE09512AAAA] *Alcatel-Lucent 7210 SAS D, E OS Services Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09512AAAA

[3HE09513AAAA] *Alcatel-Lucent 7210 SAS-M and 7210 SAS-T OS Services Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09513AAAA

[3HE09530AAAA] *Alcatel-Lucent 7210 SAS M, X, T, R6 OS MPLS Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09530AAA

[3HE09514AAAA] *Alcatel-Lucent 7210 SAS-X, R6 OS Services Guide*, Software Version: Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09514AAAA

[3HE09522AAAA] *Alcatel-Lucent 7210 SAS D, E OS System Management Guide*, Software Version Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09522AAAA

[3HE09523AAAA] *Alcatel-Lucent 7210 SAS M, T, X, R6 OS System Management Guide*, Software Version Service Access Switch Release 7.0 Rev. 01, 2014, Document Part Number: 3HE09523AAAA

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST is conformant with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, Revision 4, September 2012:

b. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012;

c. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1, Revision 4, September 2012; and

d. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1, Revision 4, September 2012.

The Target of Evaluation (TOE) for this ST is:

- CC Part 2 conformant; and
- CC Part 3 conformant.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE described by this ST does not claim conformance with any Protection Profile (PP).

2.3 EVALUATION ASSURANCE LEVEL (EAL)

This Security Target claims conformance to EAL3, 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 in Table 3 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; and

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[6] which is in keeping with the desired EAL 3+ 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.

Table 3: Threats

Identifier	Description
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.CPU_TRAFFIC	The volume of traffic, from authorized or unauthorized entities, destined to the CPUs on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS is so great that the CPU is unable to respond to legitimate traffic. This type of protection is critical at hub site or central locations where the size of nodes is processing very large amounts of data from many branch/remote locations at the central location.

[6] Attack Potential is a function of expertise, resources and motivation. Refer to Sections B.3 and B.4 of the "*Common Methodology for Information Technology Security Evaluation - Evaluation Methodology*", Document ID: CCMB-2007-09-004 for a detailed discussion of Attack Potential and how it is estimated.

Table 3: Threats

Identifier	Description
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 ORGANIZATIONAL SECURITY POLICIES

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.

Table 4 defines the Organizational Security Policies (OSPs) that are to be enforced by the TOE, its operational environment, or a combination of the two.

Table 4: Organizational Security Policies

Identifier	Description
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.

3.3 OPERATIONAL ENVIRONMENT 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 the claimed 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 made on physical, personnel and operational environment.

3.3.1 Personnel Assumptions

Table 5 identifies the assumptions made regarding the personnel who will manage and operate the TOE in its intended operating environment.

Table 5: Personnel Assumptions

Identifier	Description
A.ADMINISTRATOR	It is assumed that 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. It is further assumed that personnel will be trained in the appropriate use of the TOE to ensure security.

3.3.2 Physical Environment Assumptions

Table 6 identifies the assumptions made regarding the physical environment in which the TOE will operate.

Table 6: Physical Environment Assumptions

Identifier	Description
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.
A.LOCATION	It is assumed that the processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
A.CONNECTIVITY	It is assumed that the trusted remote systems that communicate with the TOE, except for the network traffic/data interface, are attached to the internal (trusted) network. This includes: (1) the RADIUS, TACACS+ server; (2) the SAM server; (3) system with SCP interface; (4) the SNMP, Syslog servers; and (5) the NTP server. 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.

3.3.3 Operational Assumptions

The specific conditions identified in Table 7 are assumed to exist for how the TOE is operated in its environment.

Table 7: Operational Assumptions

Identifier	Description
A.GENPURPOSE	It is assumed that 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	It is assumed that external authentication services will be available to the TOE via either RADIUS, TACACS+, or both, based on defined Internet Engineering Task Force (IETF) standards.
A.INTEROPERABILITY	It is assumed that the TOE functions with the external IT entities shown in Figure 1 and with other vendors' routers on the network and meets Request for Comments (RFC) requirements for implemented protocols.
A.TIMESTAMP	It is assumed that 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.

Table 7: Operational Assumptions

Identifier	Description
A.TRUSTED_COMM[7]	It is assumed that the Operational Environment will provide trusteed communications with the following trusted systems: SAM server, system with SCP interface/remote CLI, SNMP server. It is expected that the operational environment: a. provides the TOE with the necessary trusted interfaces. Remote management traffic (to/from the TOE) will be protected using SSH or SCP (secure copy) and remote telnet and FTP will be disabled. b. 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. c. will protect communications with remote external IT entities. The operational environment will ensure that the communication channel is logically distinct from other communication channels.

[7] SSH/SCP communications is a capability provided by the SROS; however, the underlining crypto protocols are defined outside the TOE and are part of the TOE's operation environment and are not evaluated.

4 SECURITY OBJECTIVES

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

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). Mappings of security objectives to assumptions, threats and organizational security policies, along with supporting rationale, are found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

Table 8 defines the TOE security objectives that are to be addressed by the TOE.

Table 8: TOE Security Objectives

Identifier	Description
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.CPU_PROT	The TOE will limit the amount of traffic destined to the CPM (to be processed by its CPU) on 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms using configurable limits.
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 TOE security objectives listed in Table 8, see Section 4.3.1, starting on page 40.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

4.2.1 IT Security Objectives for the Operational Environment

The IT security objectives for the environment[8] listed in Table 9 are to be addressed by the Operational Environment via technical means.

Table 9: IT Security Objectives for the Operational Environment

Identifier	Description
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_COMM	The Operational Environment: a. will provide the TOE with the necessary trusted interfaces. b. will support Secure Shell Version 2 (SSH), that is a protocol that provides a secure, connection to the router. A connection is always initiated by the client (the administrator). Authentication takes place by one of the configured authentication methods (local, RADIUS, or TACACS+). SSH allows for a secure connection over an insecure network. The remote CLI/SCP interface uses SSH. c. will support SNMPv3 for communication with SAM and SNMP servers.
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 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 SROS; 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. 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 SROS communicates are considered external IT entities that are part of the TOE's operational environment. The operational environment for the SROS requires a RADIUS or TACACS+ server and the SAM for remote administration and a Network Time Protocol (NTP) server for external time synchronization.

Table 9: IT Security Objectives for the Operational Environment

Identifier	Description
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.

4.2.2 Non-IT Security Objectives for the Operational Environment

The non-IT security objectives listed in Table 10 are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

Table 10: Non-IT Security Objectives for the Operational Environment

Identifier	Description
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.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Security Objectives Rationale Related to Threats

Table 11 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 security objectives, and that each of the TOE security objectives addresses at least one of the threats. Following this table is rationale that discusses how each threat is countered by one or more Security Objectives.

Table 11: Mapping Between Security Objectives and Threats

	Security Objective							
	O.AUDIT	**O.CPU_PROT**	**O.I&A**	**O.MANAGE**	**O.MEDIATE**	**O.TOE_ACCESS**	**OE.ADMINISTRATOR**	**OE.TIME**
T.AUDIT	X						X	X
T.CPU_TRAFFIC		X						
T.MEDIATE					X			
T.TSF_DATA				X			X	
T.UNATTENDED_SESSION						X		
T.UNAUTH_MGT_ACCESS			X					

4.3.1.1 T.AUDIT Countered Rationale

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 assists 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.

4.3.1.2 T.CPU_TRAFFIC Countered Rationale

T.CPU_TRAFFIC *The volume of traffic, from authorized or unauthorized entities, destined to the CPUs on the* 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS *platforms is so great that the CPU is unable to respond to legitimate traffic. This type of protection is critical at hub site or central locations where the size of nodes is processing very large amounts of data from many branch/remote locations at the central location.*

The O.CPU_PROT objective requires that the TOE limit the amount of traffic destined to the CPM (to be processed by its CPU) on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms using configurable limits. O.CPU_PROT requires that the TOE rate limit control traffic to protect the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms from a DoS attack.

This objective provides complete TOE coverage of the threat.

4.3.1.3 T.MEDIATE Countered Rationale

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.

4.3.1.4 T.TSF_DATA Countered Rationale

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

4.3.1.5 T.UNATTENDED_SESSION Countered Rationale

T.UNATTENDED_SESSION *A user 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.

4.3.1.6 T.UNAUTH_MGT_ACCESS Countered Rationale

T.UNAUTH_MGT_ACCESS *An unauthorized user 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 an administrator to enter a unique identifier and authentication before management access is granted.

These objectives provide complete TOE coverage of the threat.

4.3.2 Environment Security Objectives Rationale Related to Assumptions and OSPs

Table 12 provides a bi-directional mapping of Assumptions and OSPs to Security Objectives for the Operational Environment. Since the Security Objectives for the Operational Environment were derived directly from the Assumptions and OSPs 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 or OSP, that each objective is suitable to meet its corresponding assumption or OSP.

Table 12: Mapping Of Security Objectives to Assumptions and OSPs

	Security Objective											
	OE.ADMINISTRATOR	**OE.CONNECTIVITY**	**OE.EXT_AUTHORIZATION**	**OE.GENPURPOSE**	**OE.INTEROPERABILITY**	**OE.LOCATION**	**OE.PHYSICAL**	**OE.TIME**	**OE.TRUSTED_COMM**	**OE.CONSOLE**	**OE.DEPLOYED_CONFIG**	**OE.USERS**
A.ADMINISTRATOR	X											
A.CONNECTIVITY		X										
A.EXT_AUTHORIZATION			X									
A.GENPURPOSE				X								
A.INTEROPERABILITY					X							
A.LOCATION						X						
A.PHYSICAL							X					
A.TIMESTAMP								X				
A.TRUSTED_COMM									X			
P.CONSOLE										X		
P.DEPLOYED_CONFIG											X	
P.USERS												X

4.3.3 Security Objectives Summary Mapping

This section provides a consolidated summary of the two previous sections demonstrating that each organizational security policy, threat and assumption maps to no less than one security objective.

Table 13: Security Objectives Summary Map

	TOE Security Objectives						Operational Environment Security Objectives											
	O.AUDIT	O.CPU_PROT	O.I&A	O.MANAGE	O.MEDIATE	O.TOE_ACCESS	OE.ADMINISTRATOR	OE.CONNECTIVITY	OE.CONSOLE	OE.DEPLOYED_CONFIG	OE.EXT_AUTHORIZATION	OE.GENPURPOSE	OE.INTEROPERABILITY	OE.LOCATION	OE.PHYSICAL	OE.TIME	OE.TRUSTED_COMM	OE.USERS
Organizational Security Policies																		
P.CONSOLE									X									
P.DEPLOYED_CONFIG										X								
P.USERS																		X
Threats																		
T.AUDIT	X						X									X		
T.CPU_TRAFFIC		X																
T.MEDIATE					X													
T.TSF_DATA				X			X											
T.UNATTENDED_SESSION						X												
T.UNAUTH_MGT_ACCESS			X															
Assumptions																		
A.ADMINISTRATOR							X											
A.CONNECTIVITY								X										
A.EXT_AUTHORIZATION											X							
A.GENPURPOSE												X						
A.INTEROPERABILITY													X					
A.LOCATION														X				
A.PHYSICAL															X			
A.TIMESTAMP																X		
A.TRUSTED_COMM																	X	

5 EXTENDED COMPONENTS DEFINITION

There are no extended SFRs for the TOE.

6 SECURITY REQUIREMENTS

Section 6 provides security 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) that contains assurance components 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 SECURITY REQUIREMENTS PRESENTATION CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

a. Selection: Indicated by surrounding brackets and italicized text, e.g., [*selected item*]. To improve readability selections of [*none*] are generally not shown;

b. Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item]. To improve readability assignments of [none] are not shown unless doing so aids in the readability and understandability of the specified requirement;

c. Refinement: Refined components are identified by using underlining additional information, or ~~strikeout~~ for deleted text; and

d. Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_IFC.1(1), Subset Information Flow Control (Peered Policy)' and 'FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)'.

The markings are relative to the requirement statements in the Common Criteria standard.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC as summarized in Table 14.

Table 14: Summary of Security Functional Requirements

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
User Data Protection (FDP)		
	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)

Table 14: Summary of Security Functional Requirements

Class	Identifier	Name
	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)
Identification and Authentication (FIA)	FIA_AFL.1(1)	Authentication Failure Handling (Console)
	FIA_AFL.1(2)	Authentication Failure Handling (Exponential Back Off - Console)
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.5	Multiple Authentication Mechanisms
	FIA_UID.2	User Identification Before Any Action
Security Management (FMT)	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
Protection of the TSF (FPT)	FPT_STM.1	Reliable Time Stamps
Resource Utilisation (FRU)	FRU_RSA.1	Maximum quotas
TOE Access (FTA)	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User Initiated Termination
	FTA_TSE.1	TOE Session Establishment

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamps

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 successful activity of administrators;

d) Log critical network traffic;

e) Logging of successful configuration changes; and

f) Security breach logging.]

Application Note: *Log critical network traffic. Applications within the SROS 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 Section 6.2.4.4 (FMT_SMF.1 Specification of Management Functions) and Section 7.1.4.4 (Specification of Management Functions).

Security breach logging. The security event source is all events that affect attempts to breach system security such as failed login attempts or attempts to access Management Information Base (MIB) tables to which the administrator is not granted access. 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].

6.2.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FIA_UID.1 Timing of Identification

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

6.2.1.3 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

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: This SFR (FAU_SAR.1) does not apply to the syslog and session audit files.

6.2.1.4 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 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: This SFR (FAU_SAR.2) does not apply to the syslog and session audit files.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_IFC.1(1) Subset Information Flow Control (Unauthenticated Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(1) Simple Security Attributes (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].

6.2.2.2 FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(2) Simple Security Attributes (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)].

6.2.2.3 FDP_IFC.1(3) Subset Information Flow Control (Export Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(3) Simple Security Attributes (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].

6.2.2.4 FDP_IFF.1(1) Simple Security Attributes (Unauthenticated Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(1) Subset Information Flow Control (Unauthenticated Policy)

FMT_MSA.3 Static Attribute Initialization

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, MAC 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 rule set 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]; and

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 the [following additional information flow control rules:

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; and

c) Using filters and Access Control Lists (ACLs) to protect against Distributed and other DoS (D/DoS) attacks].

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 the layer 3 IP packet header specification;

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 SROS network management interfaces they will be either dropped or forwarded in accordance with the type of service, ACL, policies configured; and

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

6.2.2.5 FDP_IFF.1(2) Simple Security Attributes (Authenticated Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)

FMT_MSA.3 Static Attribute Initialization

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 username 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 rule set 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 the [following additional information flow control rules:

a) Any packet that is destined to the TOE, has to have the correct IP address assigned by the network administrator to be able to remotely operate the TOE; and

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 administrator 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; and

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.]

6.2.2.6 FDP_IFF.1(3) Simple Security Attributes (Export Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(3) Subset Information Flow Control (Export Policy)

FMT_MSA.3 Static Attribute Initialization

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

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. IP address of the SNMP trap receiver;

vi. UDP port used to send the SNMP trap;

vii. SNMPv3 used to format the SNMP notification;

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

ix. RADIUS/TACAS+ server IP address].

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].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1(1) Authentication Failure Handling (Console)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

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 occur 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].

6.2.3.2 FIA_AFL.1(2) Authentication Failure Handling (Exponential Back Off - Console)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

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 ~~the defined number of~~ one (1) unsuccessful authentication attempts has been [*met*], the TSF shall [exponentially increase the delay between subsequent login attempts].

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

6.2.3.3 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets (passwords) meet [for all users except the "admin" user, the password must meet the following:

a) a minimum length (characters): default 6 and within a range of 6-50;

b) the maximum non-hashed length shall be 20 characters;

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

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

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

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; and

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].

6.2.3.4 FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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).

6.2.3.5 FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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].

6.2.3.6 FIA_UID.2 User Identification Before Any Action

Hierarchical to: FIA_UID.1 Timing of Identification

Dependencies: No dependencies.

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).

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of*] the functions [listed in Table 15] to [the Administrator].

Table 15: Security Functions

Security Functions
Configuring Management Access
Configuring IP CPM Filters
Configuring IPv6 CPM Filters
Configuring CPM Queues on the XRS/SR/ESS
Configuring Password Management Parameters
Configuring Profiles
Configuring Administrators
Copying and Overwriting Administrators and Profiles
Configuring remote administration
Configuring Login control
Configuring RADIUS/TACACS+
Configuring CPU Protection Policies
Configuring SNMP/Syslog
Configuring NTP
Configuring Event logs

Application Note: *CSM queues are not configurable on the SAR. Similarly, CPM filters and queues are not configurable on the SAS. Refer to the application note on page 26 for additional information.*

6.2.4.2 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control, or
FDP_IFC.1 Subset Information Flow Control]
FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

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].

6.2.4.3 FMT_MSA.3 Static Attribute Initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes
FMT_SMR.1 Security Roles

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.

6.2.4.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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 6.2.4.1 FMT_MOF.1 Management of Security Functions Behaviour].

6.2.4.5 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

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

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.6 Resource Utilisation (FRU)

6.2.6.1 FRU_RSA.1 Maximum Quotas

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_RSA.1.1 The TSF shall enforce maximum quotas on the following resources: [LACP/LMI packets, control traffic per port, unconfigured protocols, control traffic per source on the CPM devices] that [*the CPM on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms*] can use [*over a specified period of time*].

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.2 FTA_SSL.4 User-initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.3 FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other components

Dependencies: No dependencies

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].

6.3 TOE SECURITY ASSURANCE REQUIREMENTS

The security assurance requirements for the TOE consist of the requirements corresponding to the EAL3 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Basic Flaw Remediation (ALC_FLR.1).

The assurance requirements for this evaluation are summarized in Table 16: EAL 3+ Assurance Requirements.

Table 16: EAL 3+ Assurance Requirements

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
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
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.4 CC COMPONENT HIERARCHIES AND DEPENDENCIES

Table 17 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.

Table 17: Functional Requirements Dependencies

SFR	Dependencies	Dependency Satisfied?
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes Yes - Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FDP_IFC.1(1)	FDP_IFF.1(1)	Yes

Table 17: Functional Requirements Dependencies

SFR	Dependencies	Dependency Satisfied?
FDP_IFC.1(2)	FDP_IFF.1(2)	Yes
FDP_IFC.1(3)	FDP_IFF.1(3)	Yes
FDP_IFF.1(1)	FDP_IFC.1(1) FMT_MSA.3	Yes Yes
FDP_IFF.1(2)	FDP_IFC.1(2) FMT_MSA.3	Yes Yes
FDP_IFF.1(3)	FDP_IFC.1(3) FMT_MSA.3	Yes Yes
FIA_AFL.1(1)	FIA_UAU.1	Yes - Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_AFL.1(2)	FIA_UAU.1	Yes - Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_SOS.1	None	N/A
FIA_UAU.2	FIA_UID.1	Yes – Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FIA_UAU.5	None	N/A
FIA_UID.2	None	N/A
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	[No Yes] Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Yes – Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FPT_STM.1	None	N/A
FRU_RSA.1	None	N/A
FTA_SSL.3	None	N/A
FTA_SSL.4	None	N/A
FTA_TSE.1	None	N/A

6.5 SECURITY REQUIREMENTS RATIONALE

6.5.1 Security Functional Requirements Rationale

Table 18 provides a bi-directional mapping of Security Functional Requirements to TOE Security Objectives. This table 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.

Table 18: Mapping of SFRs to TOE Security Objectives

Security Functional Requirement	TOE Security Objective					
	O.AUDIT	O.CPU_PROT	O.I&A	O.MANAGE	O.MEDIATE	O.TOE_ACCESS
FAU_GEN.1 Audit Data Generation	X					
FAU_GEN.2 User Identity Association	X					
FAU_SAR.1 Audit Review	X					
FAU_SAR.2 Restricted Audit Review	X					
FDP_IFC.1(1) Subset Information Flow Control (Unauthenticated Policy)					X	
FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)					X	
FDP_IFC.1(3) Subset Information Flow Control (Export Policy)					X	
FDP_IFF.1(1) Simple Security Attributes (Unauthenticated Policy)					X	
FDP_IFF.1(2) Simple Security Attributes (Authenticated Policy)					X	
FDP_IFF.1(3) Simple Security Attributes (Export Policy)					X	
FIA_AFL.1(1) Authentication Failure Handling (Console)			X			
FIA_AFL.1(2) Authentication Failure Handling (Exponential Back Off - Console)			X			
FIA_SOS.1 Verification of Secrets			X			
FIA_UAU.2 User Authentication Before Any Action			X			
FIA_UAU.5 Multiple Authentication Mechanisms			X			
FIA_UID.2 User Identification Before Any Action			X			
FMT_MOF.1 Management of Security Functions Behaviour				X		
FMT_MSA.1 Management of Security Attributes				X		
FMT_MSA.3 Static Attribute Initialization				X	X	
FMT_SMF.1 Specification of Management Functions				X		
FMT_SMR.1 Security Roles				X		
FPT_STM.1 Reliable Time Stamps	X					
FRU_RSA.1 Maximum Quotas		X				
FTA_SSL.3 TSF-initiated Termination						X
FTA_SSL.4 User-initiated Termination						X
FTA_TSE.1 TOE Session Establishment						X

The following subsections describe how each applicable TOE Security Objective is addressed by the corresponding Security Functional Requirements.

6.5.1.1 Satisfaction of O.AUDIT Rationale

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 generate audit records which will include the time that the event occurred and the identity of the administrator performing the event. [FAU_GEN.1, FAU_GEN.2, and FPT_STM.1].

The TOE will provide the privileged administrators the capability to review Audit data. [FAU_SAR.1and FAU_SAR.2].

6.5.1.2 Satisfaction of O.CPU_PROT Rationale

O.CPU_PROT *The TOE will limit the amount of traffic destined to the CPM (to be processed by its CPU) on the 7450 ESS-6/ESS-7/ESS-12, 7750 SR-7/SR-12, and 7950 XRS platforms using configurable limits.*

The TOE on the XRS/SR/ESS models will enforce maximum quotas on the LACP/LMI packets, control traffic per port, unconfigured protocols, and control traffic per source destined to the CPM over a specified period of time. [FRU_RSA.1].

6.5.1.3 Satisfaction of O.I&A Rationale

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. [FIA_UAU.5]

6.5.1.4 Satisfaction of O.MANAGE Rationale

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_MOF.1]

The TOE ensures that access to TOE security functions and configuration data is based on the assigned administrator role. [FMT_SMR.1]

6.5.1.5 Satisfaction of O.MEDIATE Rationale

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 and authenticated information flow control SFPs [FDP_IFC.1(1) and FDP_IFC.1(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(1), FDP_IFF.1(2), and FDP_IFF.1(3)]. Information that is permitted to flow will then be routed according to the information in the routing table [FDP_IFF.1(1), FDP_IFF.1(2), and FDP_IFF.1(3)].

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_IFC.1(3)]

6.5.1.6 Satisfaction of O.TOE_ACCESS Rationale

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.

6.5.2 Security Assurance Requirements Rationale

Alcatel-Lucent has decided that the TOE will be evaluated at EAL 3, augmented with basic flaw remediation (ALC_FLR.1). This combination is termed EAL 3+. This provides a level of independently assured security that is consistent with the postulated threat environment. Specification of EAL 3+ includes the vulnerability assessment component.

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 19.

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 SROS records the start-up and shutdown of the audit functions. It also generates an audit record of the following events:

a. *Log successful activity of administrators*. The SROS logs the activity of the administrator in a security log;

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

c. *Logging of successful 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; and

d. *Security breach logging*. The security event source is all events that affect attempts to breach system security such as failed login attempts or attempts to access Management Information Base (MIB) tables to which the administrator is not granted access . Security events are generated by the security application.

The SROS 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 SROS.

The SROS 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; and

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:

- *Security* - The security event source is all events that affect attempts to breach system security;
- *Change* - The change activity event source is all events that directly affect the configuration or operation of the node;
- *Debug* — The debug event source is the debugging configuration that has been enabled on the system; and
- *Main* - The main event source receives events from all other applications within the XRS/SR/ESS, SAR, and SAS-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 SROS associates the event sources with logging destinations:

- *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;
- *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;
- *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;
- *Syslog* - All selected log events are sent to the Syslog address; and
- *File* - All selected log events will be directed to a file on one of the CPM/CSM 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.
- *Console* - All selected log events will be sent to the system console.

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 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;
- *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;
- *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; and
- *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 SROS, 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 time stamp in Universal Time Co-ordinated (UTC) or local time; and
- The generating application:
  - A unique event ID within the application;
  - A router name identifying the VRF-ID that generated the event;
  - A subject identifying the affected object; and
  - A short text description.

7.1.2.2 User Identity Association

For audit events resulting from actions of identified administrators, the SROS 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:

a. Configuration Commands;

b. Show Commands; and

c. 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 SROS 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 SROS 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 views 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 an 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 SROS 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.

7.1.2.5 Reliable Time Stamps

The SROS synchronizes its local time with an NTP server in the operational environment. The SROS includes the date and time (using either UTC or local time as configured by the Administrator) within each audit record that it generates.

7.1.3 F.I&A

7.1.3.1 Authentication Failure Handling (Console)

The following is defined by the administrator:

a. The number of unsuccessful login attempts allowed for the specified time.

b. The period of time, in minutes, that a specified number of unsuccessful attempts that are made before the administrator is locked out.

c. 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:

- The SROS 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 SROS via the console; and
- When the defined number of unsuccessful authentication attempts has been met, the SROS 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 Back Off - Console)

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 tries to gain access to the SROS by using a script to try any conceivable password. SROS increases the delay between login attempts exponentially to mitigate attacks. It is applied to the console login.

The SROS 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 SROS].

7.1.3.3 Verification of Secrets

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

The password for all users except the "admin" username needs to satisfy the following requirements:

a. A minimum length (characters) default 6 and within a range of 6-50;

b. A maximum length of 56 characters;

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, one of the following flags is set, either:

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: ~!@#$%^&*() +|{}:"<>?`-=\[];',./; and

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 SROS 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 an administrator name and password combination when a administrator attempts to log in. When an administrator attempts to log in through the console, or remotely, each client (7x50 XRS/SR/ESS, 7705 SAR, and 7210 SAS) sends an access request to a RADIUS, TACACS+, or local database.

7.1.3.5 User Identification Before Any Action

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

7.1.3.6 Multiple Authentication Mechanisms

The SROS 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

The Service Aware Manager (SAM) provides GUI management functions (e.g., provisioning) for the XRS/SR/ESS, SAR, and SAS-series platforms. The SAM is defined outside the TOE boundary with a Console CLI (provides administrators with backside services) also outside the TOE boundary. All of the routers and switches listed in Table 2 can be managed by the 5620 SAM. The SAM includes the Element Manager (SAM-E), Provisioning (SAM-P), and Assurance (SAM-A) modules.

The SROS 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 SROS 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.

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 an 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 CPM filters and queues that control all traffic going in to the CPM, including all routing protocols for the 7x50 XRS/SR/ESS and 7705 SAR-series platforms;

e. Configures CSM filters and queues that control all traffic going in to the CSM, including all routing protocols for the 7x50 XRS/SR/ESS-series platforms;

f. Configures authentication attempts count, time interval [minutes], and lockout time period [minutes];

g. Configures authentication-order for local console, RADIUS and TACACS+;

h. Configures password complexity [numeric] [special-character] [mixed-case];

i. Configures password minimum-length value;

j. Configures: management access filters, profiles, administrator access parameters, password management parameters;

k. Enables RADIUS and/or TACACS+ (TOE client-side);

l. Configures event and logs;

m. Configures access parameters for individual administrators - the login name for the administrator and information that identifies the administrator;

n. Configures administrator profiles used to deny or permit access to CLI command tree permissions, or specific CLI commands;

o. Copies a profile or administrator or overwrite an existing profile or administrator;

p. Allows/disallows a administrator the privilege to change their password for console login; and

q. Configure the CPU protection global and interface-specific (in CPU protection profiles) configuration limits.

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; and

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. Show Commands;

o. Security Commands;

p. Login Control;

q. Clear Commands;

r. Authentication Commands;

s. CPU Protection Commands; and

t. 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

7.1.4.2.1 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.

7.1.4.2.2 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;

e. configures the idle timeout for file-copy, console, or remote sessions which determines when the session is terminated by the system; and

f. Configures Management Access Filters to control all traffic in and out of the SROS and to restrict management of the SROS 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.

7.1.4.2.3 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); and

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:

(1) Set of destination network identifiers;

(2) Syslog server IP address;

(3) UDP port used to send the syslog message;

(4) Syslog Facility Code;

(5) Syslog Severity Threshold; and

(6) Port number used to send SNMP traffic.

7.1.4.3 Static Attribute Initialization

SROS 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 SROS requires local console access to initially configure an IP address and enable remote access.

Administrators are set up 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 SROS:

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; and

h. security management functions listed in Section 7.1.4.1.

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; and

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

The SROS implements the periodic backup of the SROS 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 SROS 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 role associated with the SROS: 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 SROS 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 SROS 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 SROS allows configuring login control parameters for console and remote administration sessions.

The SROS has the ability to terminate stale (inactive) connections. The SROS 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.

Administrators initiate termination of their own sessions. The SROS allows an administrator to terminate their own session by issuing the command "logout" at the CLI prompt.

7.1.5.3 TOE Session Establishment

The SROS will deny session establishment after an administrator defined number of active SAM sessions thereby limiting the number of inbound SAM sessions. The SROS 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 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.

7.1.6.2 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.

7.1.6.3 Subset Information Flow Control (Export Policy)

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

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

7.1.6.4 Simple Security Attributes (Unauthenticated Policy)

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

The administrator configures the SR-series routers, ESS-series switches, SAR-series routers, and SAS-series switches setting the following protocols, standards, and services from the set of:

a. OSPFv2;

b. IS-IS;

c. BGP-4; and

d. MPLS (LDP, RSVP-TE).

The 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 SROS 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.

For the XRS/SR/ESS-series platforms, 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 7705 SAR CSM queues and 7210 SAS CPM filters and queues are not configurable. These mechanisms are fixed in terms of usage (i.e., each queue handles a specific type of traffic) and configuration (i.e., each queue is configured for specific rates and buffering capacities). To avoid DoS-like attacks overwhelming the Control Plane, while ensuring that critical control traffic (such as signalling) is always serviced in a timely manner, the 7705 SAR has three queues (High, Low, and Ftp) for handling packets addressed to the CSM:

- High: handles all messaging this is important for keeping the network stable from a control plan point of view. The messages in this queue are related to network management, signalling, routing, etc.;
- Low: handles messages that can be treated with a lower importance when doing so has no detrimental impact on the overall stability of the network. Examples include ICMP ECHO REQ (pings), etc.; and
- Ftp: handles messages related to bulk file transfers. These types of messages require appropriate buffering with little or no CSM interference. Examples include the ftp download of a new software image, etc.

Packets that are destined to the 7210 SAS CPU are prioritized based on the application. These include Layer 2 data packets (a copy of which is sent to CPU for MAC learning), EFM, CFM, STP, LACP, ICMP, etc. The CPU provides eight queues from BE (0) to NC (7). Packets destined to the CPU are classified internally and are put into the correct queue. These packets are rate-limited to prevent DoS attacks. The software programs the classification entries to identify these packets and assigns appropriate bandwdith and priority to them. As noted above, 7210 SAS CPM filters are not configurable by the user.

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; and

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 SROS 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.

7.1.6.5 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:

a. source port and IP protocol ID and address;

b. username/password and profile;

c. source network identifier;

d. remote or console session idle timeout;

e. maximum number of concurrent inbound remote sessions;

f. administrator permission for remote or console access; and

g. local home directory for the administrator for remote or console access.

Destination subject security attributes are:

a. set of destination subject identifiers (UDP/TCP port number).

Any packet that is destined to the SROS, has to have the correct IP address that has been assigned by the network administrator to be able to remotely operate the SROS. Once the packet has been identified to be forwarded to the CPM/CSM, it is put under the influence of the CPM/CSM filters.

Management Access Filters (MAFs) control all traffic to the CPM on the XRS/SR/ESS and SAS-series devices as well as all routing protocols. Functionally equivalent filtering is provided by the CSM filters on the SAR-series devices. For SAR-series devices, MAFs also control all traffic in and out of the CSM. They can be used to restrict management of the SAR by other nodes outside specific (sub)networks or through designated ports.

MAFs apply to packets from all ports to restrict management of the SROS from other nodes who are unauthorized. MAFs / CSM filters restrict access to the SROS to small list of SAM servers or support workstations. MAFs / CSM filters control all traffic going into the CPM/CSM, including all routing protocols. They apply to packets from all ports. The filters are used to restrict management of the router or 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 or CSM filter and their entries must be explicitly created on each router. These filters apply to the management Ethernet port. MAFs / CSM filters 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.

7.1.6.6 Simple Security Attributes (Export Policy)

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

Subject and information security attributes used are:

a. Source subject security attributes: source network identifier; and

b. Destination subject security attributes:

(1) Syslog server IP address;

(2) UDP port used to send the syslog message;

(3) Syslog Facility Code;

(4) Syslog Severity Threshold;

(5) IP address of the SNMP trap receiver;

(6) UDP port used to send the SNMP trap;

(7) SNMPv3 used to format the SNMP notification;

(8) Security name and level for SNMPv3 trap receivers; and

(9) RADIUS/TACACS+ server IP address.

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 SROS.

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

7.1.7.1 Maximum Quotas

The SROS on the XRS/SR/ESS provides rate limiting mechanisms to protect the CPM processing resources of its router. CPU protection protects the CPU of the node from a DoS attack by limiting the amount of traffic coming in from one of its ports and destined to the CPM using a combination of configuration limits. Some configuration limits are configured globally for the node and other limits are configured in CPU protection profiles which are assigned to interfaces.

The following limits are available to be configured globally for the node:

- link-specific rate – applies to the link-specific protocols LACP (Ethernet LAG control) and LMI (ATM, Ethernet, and Frame Relay);
- port-overall rate – applies to all control traffic to each port; and
- protocol-protection – blocks network control traffic for unconfigured protocols.

The following limits are available to be configured within CPU protection profiles which are assigned to interfaces:

- overall-rate – Applies to all control traffic destined to the CPM received on the specified interface. Control traffic received above this rate will be discarded;
- per-source rate – Used to limit control traffic destined to the CPM from each individual source. This per-source-rate is only applied when an object (Service Access Point (SAP)) is configured with a cpu-protection policy and also with the optional mac-monitoring or ip-src-monitoring keywords. A source is defined as a *SAP* with *Source MAC Address* tuple for mac-monitoring or as a *SAP* with *Source IP Address* tuples for **ip-src**-monitoring. Only certain protocols (as configured under *included-protocols* in the cpu protection policy) are limited (per source) when the **ip-src**-monitoring keyword is used; and

- out-profile-rate –Applies to all control traffic destined to the CPM received on the specified interface. Control traffic received above this rate will be marked as eligible to be discarded and is more likely to be discarded if there is contention for CPU resources.

7.2 TOE SECURITY FUNCTIONS RATIONALE

Table 19 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 7.1.

Table 19: Security Functions to SFR Mapping

Security Functional Requirement	F.Audit	F.I&A	F.Security_Management	F.TOE_Access	F.User_Data_Protection	F.TSF_Protection
FAU_GEN.1 Audit Data Generation	X					
FAU_GEN.2 User Identity Association	X					
FAU_SAR.1 Audit Review	X					
FAU_SAR.2 Restricted Audit Review	X					
FDP_IFC.1(1) Subset Information Flow Control (Unauthenticated Policy)					X	
FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)					X	
FDP_IFC.1(3) Subset Information Flow Control (Export Policy)					X	
FDP_IFF.1(1) Simple Security Attributes (Unauthenticated Policy)					X	
FDP_IFF.1(2) Simple Security Attributes (Authenticated Policy)					X	
FDP_IFF.1(3) Simple Security Attributes (Export Policy)					X	
FIA_AFL.1(1) Authentication Failure Handling (Console)		X				
FIA_AFL.1(2) Authentication Failure Handling (Exponential Back Off - Console)		X				
FIA_SOS.1 Verification of Secrets		X				
FIA_UAU.2 User Authentication Before Any Action		X				
FIA_UAU.5 Multiple Authentication Mechanisms		X				
FIA_UID.2 User Identification Before Any Action		X				
FMT_MOF.1 Management of Security Functions Behaviour			X			
FMT_MSA.1 Management of Security Attributes			X			
FMT_MSA.3 Static Attribute Initialization			X			
FMT_SMF.1 Specification of Management Functions			X			
FMT_SMR.1 Security Roles			X			
FPT_STM.1 Reliable Time Stamps	X					
FRU_RSA.1 Maximum Quotas						X
FTA_SSL.3 TSF-initiated Termination				X		
FTA_SSL.4 User-initiated Termination				X		
FTA_TSE.1 TOE Session Establishment				X		

8 OTHER REFERENCES

This section lists references other than the TOE guidance documentation presented in Section k on page 27 that either aid in better understanding the TOE or are referred to directly in this Security Target.

[ANSI X3.64] *Additional Controls for Use with the American National Standard Code for Information Interchange*, ANSI X3.64-1979(R1990), American National Standards Institute (ANSI)

[IEEE 802.3ad] *Amendment to Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications-Aggregation of Multiple Link Segments*, IEEE Standard 802.3ad-2000, Institute of Electrical and Electronic Engineers

[RFC 1305] *Network Time Protocol (Version 3) Specification, Implementation and Analysis*, RFC 1305, March 1992, Internet Engineering Task Force

[RFC 1492] *An Access Control Protocol, Sometimes Called TACACS*, RFC 1492, July 1993, Internet Engineering Task Force

[RFC 2138] *Remote Authentication Dial In User Service (RADIUS)*, RFC 2138, April 1997, Internet Engineering Task Force

[RFC 2865] *Remote Authentication Dial In User Service (RADIUS)*, RFC 2865, June 2000, Internet Engineering Task Force

[RFC 2866] *RADIUS Accounting*, RFC 2866, June 2000, Internet Engineering Task Force

[RFC 3411] *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, RFC 3411, December 2002, Internet Engineering Task Force

[RFC 3412] *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*, RFC 3412, December 2002, Internet Engineering Task Force

[RFC 3413] *Simple Network Management Protocol (SNMP) Applications*, RFC 3413, December 2002, Internet Engineering Task Force

[RFC 3414] *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, RFC 3414, December 2002, Internet Engineering Task Force

[RFC 3415] *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, RFC 3415, December 2002, Internet Engineering Task Force

[RFC 3416] *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*, RFC 3416, December 2002, Internet Engineering Task Force

[RFC 3417] *Transport Mappings for the Simple Network Management Protocol (SNMP)*, RFC 3417, December 2002, Internet Engineering Task Force

[RFC 3418] *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*, RFC 3418, December 2002, Internet Engineering Task Force

[RFC 4250] *The Secure Shell (SSH) Protocol Assigned Numbers*, RFC 4250, January 2006, Internet Engineering Task Force

[RFC 4251] *The Secure Shell (SSH) Protocol Architecture*, RFC 4251, January 2006, Internet Engineering Task Force

[RFC 4252] *The Secure Shell (SSH) Authentication Protocol*, RFC 4252, January 2006, Internet Engineering Task Force

[RFC 4253] *The Secure Shell (SSH) Transport Layer Protocol*, RFC 4253, January 2006, Internet Engineering Task Force

[RFC 4254] *The Secure Shell (SSH) Connection Protocol*, RFC 4254, January 2006, Internet Engineering Task Force

[RFC 5424] *The Syslog Protocol*, RFC 5424, March 2009, Internet Engineering Task Force

[TIA-232-F] *Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, October 1 1997, Telecommunications Industry Association (TIA)