Swedish Certification Body for IT Security

Certification Report- Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family

Issue: 1.0, 2015-aug-28

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The TOE is the Alcatel-Lucent 7-Series Service Router Operating System (SROS) Software consisting of the:

- Alcatel-Lucent 7x50 Service Router Operating System (SR OS), v12.0. The specific build number is 12.0R4.
- Alcatel-Lucent 7705 Service Aggregation Router Operating System (SAR OS), v6.1 The specific build number is 6.1R4.
- Alcatel-Lucent 7210 Service Access Switch Operating System (SAS OS), v7.0. The specific build number is 7.0R1.

The TOE consists of the SROS software running on various router and switch platforms and models, and Control Processor Module (CPM) and Control and Switching Module (CSM) hardware queues associated with the various platforms and models.

For information about features excluded from the TOE Evaluated Configuration, see section 8.2 below.

The evaluation has been performed by Combitech AB and EWA-Canada. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL3, augmented by ALC_FLR.1 Flaw reporting procedures.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

EWA-Canada operates as a Foreign location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 3 + ALC_FLR.1.

2 Identification

Certification Identification	
Certification ID	CSEC2014006
Name and version of the certified IT product	Alcatel-Lucent 7-Series Service Router Operating (SROS) Family
Security Target Identification	Security Target for the Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family, Issue 0.14, 2015-06-16
EAL	EAL3+ALC_FLR.1
Sponsor	Alcatel-Lucent Inc.
Developer	Alcatel-Lucent Inc.
ITSEF	Combitech AB and EWA-Canada, Ltd.
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification completion date	2015-08-18

3 Security Policy

The TOE consists of six security functions. Below is a short description of each of them. For more information, see Security Target [ST].

3.1 F.Audit

Functionality for audit data generation, user identity association, audit review, restricted audit review, and reliable time stamps.

3.2 F.I&A

Functionality for authentication failure handling, verification of secrets, user authentication before any action, user identification before any action, and multiple authentication mechanisms.

3.3 F.Security_Management

Functionality for management of security functions behaviour, management of security attributes, static attribute initialization, specification of management functions, and security roles.

3.4 F.TOE_Access

Functionality for TSF-initiated termination, user-initiated termination, and TOE session establishment.

3.5 F.User_Data_ Protection

Functionality for subset information flow control and simple security attributes.

3.6 F.TSF_Protection

Functionality for maximum quotas.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] describes one usage assumption.

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.

4.2 Environmental Assumptions

The Security Target [ST] describes eight environmenal assumptions.

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.

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.

A.TRUSTED_COMM It is assumed that the Operational Environment will provide trusted 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.

4.3 Clarification of Scope

The threat agents are divided into two categories:

- 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
- 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.

The identified threats against the TOE are listed below:

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.

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.

There are three Organisational Security Policies (OSPs) - these are listed below:

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.

5 Architectural Information

5.1 TOE Design

The TOE consists of software and the hardware queues for the 7x50 and 7210 platforms, the Control Processor Module - CPM, the hardware queues for the 7705 platform, and the Control and Switching Module - CSM.

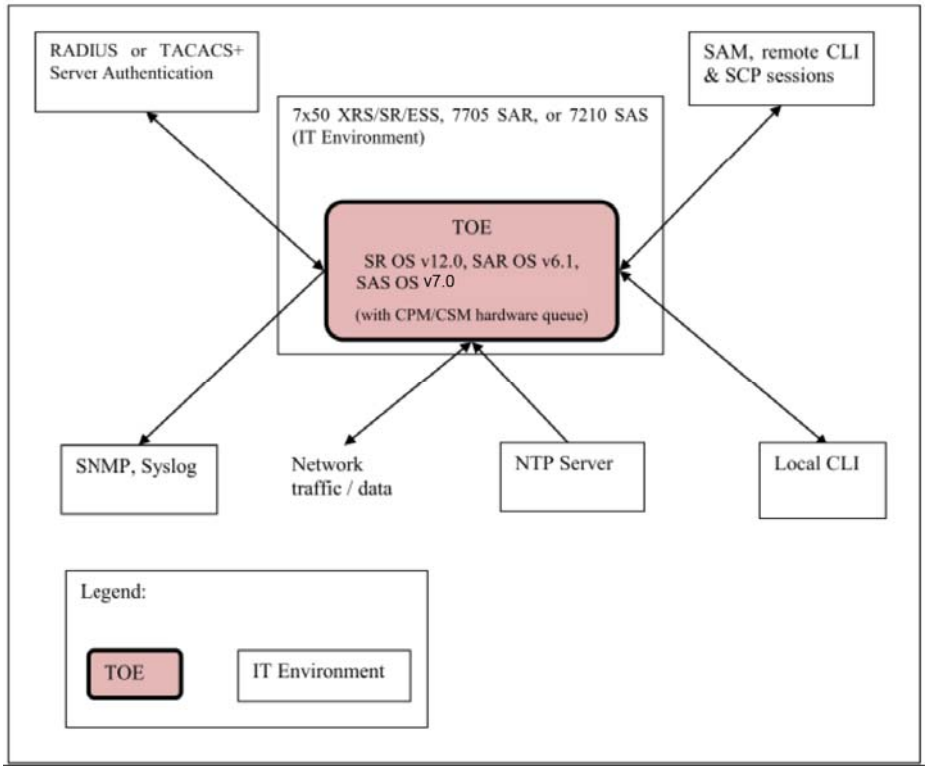

Figure 1 TOE Boundary

The physical boundary is the SROS operating system (i.e., SR OS v12.0, SAR OS v6.1, and 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.

The TOE is comprised of the following subsystems:

- Management Plane subsystem, SFR-Enforcing – provides configuration control and the connection of statistics and state information for reporting. This subsystem includes Authentication, Authorization, and Accounting, CLI, SNMP, and Logging modules;

- Control Plane subsystem, SFR-Enforcing – handles the dynamic protocols for the exchange of (reachability, topological, and resource state) information, allowing for an accurate forwarding operation, Control Plane Protection. The Control Plane performs access decisions on control and management traffic (CPM/CSM filter and MAF) and implements routing and MPLS protocols.
- Data Plane subsystem, SFR-Enforcing – handles the forwarding of customer data or service data through the system and provides other planes with statistics and state information, Data Plane Protection. The Data Plane implements QoS policies, ACL policies, and Filter policies.
- Platform subsystem, SFR-Supporting – manages the overall hardware system (chassis management) and provides the basic tools for other subsystems to obtain information and communicate with other subsystems as well as the interaction with outside elements.

6 Documentation

The guidance documentation that accompanies the TOE is listed in the following sub-sections.

6.1 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 Guide5, Services Guide Release 12.0 Release 4, Alcatel-Lucent Document Part Number: 93-0107-11-01 Edition 01, 2014[1]

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

6.2 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

6.3 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
[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

7 IT Product Testing

7.1 Developer Tests

The developer performed both manual tests and run automatic tests suites. The developer's testing covers the security functional behaviour of all TSFIs and SFRs as well as the interactions of the subsystems.

The evaluator's independent tests were chosen to complement the developer's manual tests in covering as much as possible of the security functional behavior of the TSFIs and SFRs.

The evaluator repeated two (one partly) of the developer's automatic tests script suites, two of the developer's manual test cases and performed the independent and penetration test cases. The tests included:

- TOE installation
- Configuring NTP
- RADIUS authentication
- Traffic filters
- SNMP trap target
- CPM traffic limitation

The evaluator used the same test-bed as the developer, which is a network with six nodes. A test-bed server contains the auto-test environment, the test scripts, and a variety of tools that were used for testing (i.e. DHCP server, RADIUS server, TACACs server, SNMP agent, etc.). A traffic generator (IXIA) is also connected as well as terminal servers, hubs, IP-controlled power bars, etc. The network is fully meshed, i.e. each node is cabled to every other node, with multiple parallel links between a sub-set of nodes. Similar test-beds are used for all TOE families.

Tests were run manually from the test-bed server, a terminal server for remote CLI interaction and an external laptop. Automatic test scripts were also run from the test-bed server and the results, Pass/Fail, were examined in the regression test database.
The actual results of all test cases were consistent with the expected test results and all tests were judged to pass.

7.2 Penetration Tests

Three types of penetration tests were executed:

- Port scanning
- Vulnerability scanning
- Communication protocol compliance

Port scans were run after installation and configuration had been done according the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned for TCP/UDP.

Nessus (www.tenable.com) basic network vulnerability scans were run. No high severity issues were found.

It was verified that the SSHv2 channel was encrypted and that no older versions of the protocol could be used.

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

8.1 Dependencies to Other Hardware, Firmware and Software

The TOE runs on the router and switch platforms and models listed in table 1 The hardware for the models listed in table 1is 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.

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

Table 1

8.2 Excluded from the TOE 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.

- 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.
- 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.

- 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.
- 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.

- The use of Telnet and FTP is not allowed in the evaluated configuration.
- The use of the Netconf server is not allowed in the evaluated configuration.
- The use SNMPv1 and SNMPv2 are not allowed in the evaluated configuration.
- The use of SSHv1 is not allowed in the evaluated configuration.
- 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.

9 Results of the Evaluation

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	Pass
ST Introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security Problem Definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Authrisation controls	ALC_CMC.3	Pass
Implementation representation CM coverage	ALC_CMS.3	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Flaw reporting procedure	ALC_FLR.1	Pass
Development	ADV	Pass
Security Architecure description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.3	Pass
Architecual design	ADV_TDS.2	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: Basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Vulnerability analysis	AVA_VAN.2	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
CC	Common Criteria
TOE	Target of Evaluation
PP	Protection Profile
SFR	Security Functional Requirements
SAR	Security Assurance Requirements
TSF	TOE Security Functions
OR	Observation Reports
SER	Single Evaluation Report
FER	Final Evaluation Report
7210	A collective term used in this document to refer to Alcatel-Lucent 7210 SAS service access switches.
7705	A collective term used in this document to refer to Alcatel-Lucent 7705 SAR service aggregation routers.
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.
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.

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 peer-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 software 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 .
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.
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.
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	A Service Access Point (SAP) identifies the customer interface point

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.
Service Aggregation Router	Service Aggregation Router (SAR) is a collective term used in this document to refer to the four 7705 SAR router models.
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. 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.
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.
SRc	SRc is a collective term used in this document to refer to Alcatel-Lucent 7750 SRc service routers.
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.

12 Bibliography

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[SP-002] Evaluation and Certification, SP-002, Issue: 22.0, 2014-12-12, 14FMV9859-38:1, FMV/CSEC

[ST] Security Target for the Alcatel-Lucent 7-Series Service Router Operating System (SROS) Family, Issue 0.14, 2015-06-16

Appendix A QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2014-05-21:

QMS 1.16.1 valid from 2014-03-27

QMS 1.16.2 valid from 2014-07-07

QMS 1.17 valid from 2014-11-20

QMS 1.17.1 valid from 2014-12-02

QMS 1.17.2 valid from 2015-01-13

QMS 1.17.3 valid from 2015-01-29

QMS 1.18 valid from 2015-06-18

QMS 1.18.1 valid from 2015-08-21

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista QMS 1.18.1”.

The certifier concluded that, from QMS 1.16.1 to the current QMS 1.18.1, there are no changes with impact on the result of the certification.