Alcatel-Lucent Enterprise OmniSwitch with AOS 8.6.R11 Security Target for EAL2

Version:	**3.2**
Part Number:	**014565-01**
Status:	**Final**
Last Update:	**2021-02-03**
Classification:	**Public**

Trademarks

atsec® is a trademark of atsec information security corporation in the United States, other countries, or both.

Omniswitch® is a trademark used by ALE USA Inc.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
3.2	2021-02-03	Alejandro Masino	Final release

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	Alcatel-Lucent Enterprise OmniSwitch with AOS 8.6.R11 Security Target for EAL2
Version:	3.2
Part Number:	014565-01
Status:	Final
Date:	2021-02-03
Sponsor:	ALE USA Inc.
Developer:	ALE USA Inc.
Keywords:	ALE USA Inc., ALE, Alcatel-Lucent Enterprise, OmniSwitch, Alcatel-Lucent Operating System, AOS, OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900, OmniSwitch 9900, OS6465, OS6560, OS6860, OS6865, OS6900, OS9900

1.2 TOE Identification

The TOE is Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.4.R11.

1.3 TOE Type

The TOE type is network switch.

1.4 TOE Overview

The Target of Evaluation (TOE) is a network switch comprised of hardware, firmware and guidance documentation.

The firmware is named Alcatel-Lucent Operating System (AOS) which is the single purpose operating system that operates the management functions of all of the Alcatel-Lucent Enterprise OmniSwitch switches. The evaluation covers AOS 8.6.4.R11, based on the Linux version 3.10.104 operating system.

Note: *The title of this Security Target, as well as related guidance documentation, refers to the TOE as AOS 8.6.R11; this label should be considered equivalent to the version of the TOE (AOS 8.6.4.R11).*

The TOE hardware consists of the following families/series.

Family / Series	AOS Version	Main Processor
OmniSwitch 6465 (OS6465)	AOS 8.6.4.R11	ARM Cortex-A9
OmniSwitch 6560 (OS6560)	AOS 8.6.4.R11	ARM Cortex-A9
OmniSwitch 6860 (OS6860)	AOS 8.6.4.R11	ARM Cortex-A9
OmniSwitch 6865 (OS6865)	AOS 8.6.4.R11	ARM Cortex-A9
OmniSwitch 6900 (OS6900)	AOS 8.6.4.R11	NXP MPC8572
		NXP QorIQ P2040
		Intel Atom C2538
OmniSwitch 9900 (OS9900)[1]	AOS 8.6.4.R11	Intel Atom C2518

Table 1: TOE Hardware Configurations

The TOE provides Layer-2 switching, Layer-3 routing, and traffic filtering. Layer-2 switching analyzes incoming frames and makes forwarding decisions based on information contained in the frames. Layer-3 routing determines the next network point to which a packet should be forwarded toward its destination. These devices may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include Border Gateway Protocol (BGP), Routing Information Protocol (RIP) v.2, and Open Shortest Path First (OSPF). Filtering controls network traffic by controlling whether packets are forwarded or blocked at the TOE’s interfaces. Each packet is examined to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

The Alcatel-Lucent Enterprise OmniSwitch 6465 Series switches are a family of hardened, compact, fan-less gigabit Ethernet switches that have been designed specifically for industrial applications. These switches are designed to operate in extended temperatures, offer higher EMI/EMC tolerance, a flexible range in power inputs options and high surge protection.

The Alcatel-Lucent Enterprise OmniSwitch 6560 Series switches are stackable Gigabit and Multi-Gigabit Ethernet LAN switches family designed for enterprise networks. The switches offer multi-gigabit ports for high-speed IEEE 802.11ac devices, 10 GigE uplinks and 20 GigE stacking.

The Alcatel-Lucent Enterprise OmniSwitch 6860 Series are stackable LAN switches that are compact, high-density GigE and 10 GigE platforms designed for the most demanding converged networks. They provide Quality of Service (QoS), access control lists (ACLs), Layer-2 / Layer-3 switching, virtual LAN (VLAN) stacking and IPv6.

The Alcatel-Lucent Enterprise OmniSwitch 6865 Series are stackable LAN switches that are compact, industrial-grade, high-density GigE and 10 GigE platforms designed to operate reliably in severe temperatures, as well as harsh physical and electrical conditions. They provide QoS, ACLs, Layer-2 / Layer-3 switching, VLAN stacking and IPv6.

[1] This model uses Network Inteface (NI) cards that include an Intel Atom C2338 processor, but does not execute any cryptographic functionality claimed in this Security Target.

The Alcatel-Lucent Enterprise OmniSwitch 6900 Series are stackable LAN and data center switches that are compact, high-density 10 GigE and 40 GigE platforms. They provide Virtual Extensible Local Area Network (VXLAN), OpenFlow, Shortest Path Bridging (SPB), Data Center Bridging (DCB) capabilities, QoS, Layer-2 and Layer-3 switching, as well as system and network level resiliency.

The Alcatel-Lucent Enterprise OmniSwitch 9900 Series are modular LAN chassis platform, high-capability, and high-performance modular Ethernet LAN switches for enterprise, service provider and data center environments. They provide uninterrupted network uptime with non-stop Layer-2 and Layer-3 forwarding. They also provide the capability to optimize/simplify Layer-2 and Layer-3 network designs, and reduce administration overhead while increasing network capacity with resilient multipath active-active dual homing multi-chassis support.

1.4.1 Intended method of use

The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only security administrators are to have access to connect to the serial console, or gain physical access to the hardware. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

The TOE is not intended for use as a general purpose computer and only executes the services needed to perform its intended function.

1.4.2 Major security features

The TOE provides the following security functions.

- Generation of audit records for security related events, which can be locally stored or sent to a remote server.
- Cryptographic support for protecting TOE Security Functionality (TSF) data, password storage, trusted update of the TOE firmware, self-tests, and for establishing secure protocols used by the TOE.
- Identification and authentication of Security Administrators that access the TOE for Security Management purposes.
- Identification and Authentication of end users and devices that connect to the TOE for sending and receiving network traffic.
- Traffic mediation, enforcing the control of inbound and outbound information flow between the TOE and other devices in the network.
- Security management of the TSF, via a Command Line Interface (CLI) using local and remote sessions, or the use of the SNMPv3 protocol.
- Protection of the TSF, through the establishment of secure channels between the TOE and external IT entities, remote consoles or other devices in the network; protection of passwords stored in the TOE; updates of the TOE firmware using trusted product updates; and provision of reliable timestamps.

1.5 TOE Description

1.5.1 Architecture

The following diagram shows the basic components that comprise the TOE.

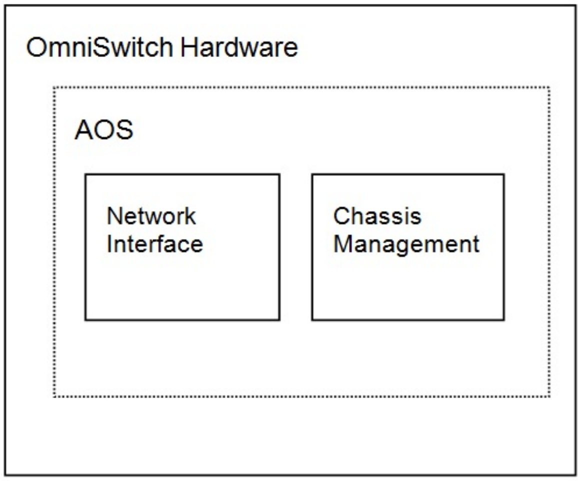

Figure 1: TOE Architecture

The term Chassis Management Module (CMM) is used to describe the logical management functionality of the TOE providing the following services.

- Console, Universal Serial Bus (USB), and Ethernet management port connections. The console port that is used to connect a serial console to initialize and configure the TOE via a Command Line Interface (CLI). Depending on the TOE model the physical interface can be an USB or an RJ-45 connector.
- Software and configuration management, including the CLI.
- Power distribution.
- Diagnostics.
- Cryptographic functionality.
- Important availability features, including failover (when used in conjunction with another CMM), software rollback, temperature management, and power management.

Network Interface (NI) modules provides the connectivity to the network through different physical ports, connector types and speed. The NI modules are categorized into Gigabit Ethernet Network Interface (GNI), 10-Gigabit Ethernet Network Interface (XNI) and 40-Gigabit Ethernet Network Interface (QNI) modules. GNI modules provide 1000 Mbps (1 Gbps) connections. GNI modules can be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media. XNI modules provide up to six 10000 Mbps (10 Gbps) connections per module and can be used in networks where 10-gigabit Ethernet is used as the backbone media. Finally, QNI modules provide 40000 Mbps (40 Gbps) connections per module.

The main distinction between models are the form factor (either chassis or stacks), the processor used, the number of physical ports, the port speeds, the connector types, and the amount of physical RAM installed.

The OS6465, OS6560, OS6860, OS6865 series products are packaged in a single PCB with an embedded CPU Cortex ARM 9 processor. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP.

The OS6900 series products are packaged in a single PCB with a NXP MPC8572, NXP QorIQ P2040 or Intel Atom C2538 processor, depending on the model. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP.

The OS9900 is a chassis based product including a CMM with an Intel Atom C2518 processor. The CMM functions execute on this processor and communicate with the NIs via a socket based protocol running over TCP/IP. This product can support up to six NI cards containing an Intel Atom C2338 processor, where the NI functions execute.

More specific information about the capabilities of each Omniswitch model can be found in Table 2.

An Omniswitch can operate in two different modes: Standalone and Virtual Chassis (VC). A virtual chassis is a group of switches managed through a single management IP address that operates as a single bridge and router. Virtual chassis connects two or more physical stackable switches through Virtual Fabric Links (VFL) and has a specific protocol to communicate between switches.

Virtual Chassis mode is not allowed in the evaluated configuration. The TOE must always operate in Standalone mode.

1.5.2 TOE boundaries

1.5.2.1 Physical

Figure 2 shows a depiction of the TOE and its operating environment. The red dotted lines enclose the TOE physical boundary.

The TOE is located between the external and the internal network of an organization in order to perform Layer-2 switching, Layer-3 routing, and traffic filtering of flowing IP packets. The TOE can be also connected to the following external IT entities:

- Administrators log onto the TOE and perform management functions via a Command Line Interface (CLI). These activities can be performed via a **Serial Console** connected to the TOE via a dedicated port, or using a **SSHv2 client** from a computer connected to the security management network.
- Administrators can also transfer information securely from and to the TOE using a **SFTP client** via the SSHv2 protocol.
- Administrators can also execute commands from the CLI to connect to external **SSH and/or SFTP servers** via the SSHv2 protocol.
- Administrators can also perform management functions using an **SNMP Management Station** connected to the security management network via the SNMPv3 protocol and protected under the Transport Layer Security (TLS) protocol.
- TOE audit records can be optionally stored in a **Syslog Server**. Communication is protected by the TLS protocol.
- The TOE can optionally perform Identification and Authentication of users using credentials stored in an external **LDAP Server**. The TOE can also request external authentication using a **RADIUS Server**. In both cases, communication is protected by the TLS protocol.
- If the TOE is part of a network where network addresses are assigned dynamically, a **Dynamic Host Configuration Protocol (DHCP) server** is required to perform this functionality.

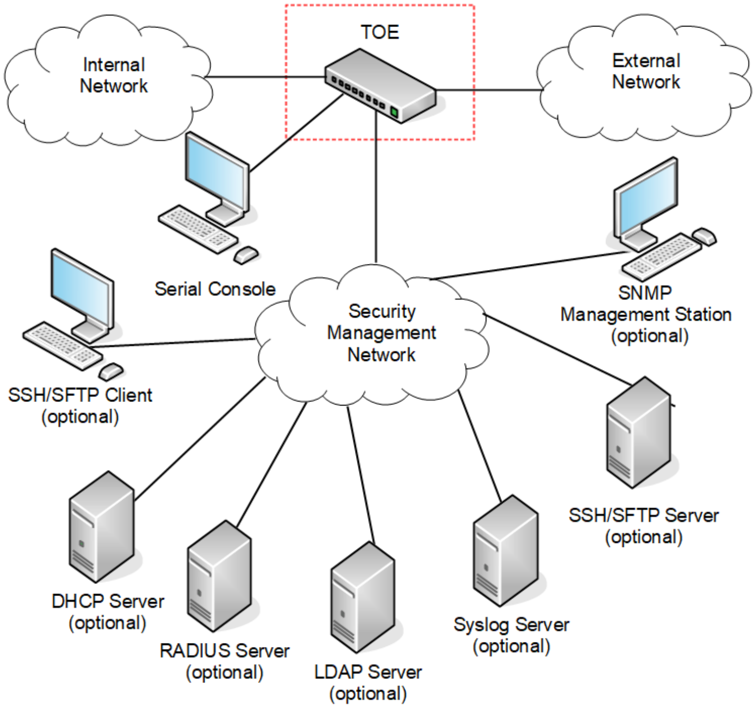

Figure 2: TOE Boundary

1.5.2.1.1 Hardware / Firmware Components

Table 2 below specifies the TOE hardware components, all of them using AOS 8.6.4.R11 as the TOE firmware. Please notice that the acronym SFP is referring to Small Form Factor Pluggable transceivers; this should not be confused with the same CC acronym that refers to Security Function Policies.

Family Series	Hardware ID	Processor	Description
OmniSwitch 6465	OS6465-P6	ARM Cortex-A9	Hardened GigE fixed configuration fan-less din-mount chassis Includes 4 RJ-45 10/100/1000 Base-T PoE+ ports out of which 2 ports are 60W PoE capable, 2 100/1000 Base-X SFP ports, RS-232 Console (RJ45), 1 Alarm relay Input, 1 alarm relay output and USB port.
	OS6465-P12	ARM Cortex-A9	Hardened GigE fixed configuration fan-less din-mount chassis. Includes 8 RJ-45 10/100/1000 Base-T PoE+ ports out of which 4 ports are 60W PoE capable, 4 100/1000 Base-X SFP ports, RS-232 Console (RJ45), 1 Alarm relay Input, 1 alarm relay output and USB port.

Family Series	Hardware ID	Processor	Description
	OS6465-P28	ARM Cortex-A9	Hardened GigE L3 fixed configuration fan-less chassis. Includes 22 10/100/1000 Base-T PoE+ ports out of which 8 ports are 60W PoE capable, two 100/1000 Base-X SFP ports, four (1G/10G) SFP+ ports, RS-232 Console (RJ45), 1 Alarm relay Input, 1 alarm relay output and one USB port.
	OS6465T-P12	ARM Cortex-A9	GigE fixed configruation chassis. Includes 8 RJ45 10/100/1000 BaseT, 2 SFP/RJ45 combo, 2 SFP ports. 1RU by 1/2 rack width, internal AC PSU.
	OS6465T-12	ARM Cortex-A9	GigE fixed configuration chassis. Includes 8 RJ45 10/100/1000 BaseT PoE+, 2 SFP/RJ45 combo, 2 SFP ports. 1RU by 1/2 rack width, internal AC PSU.
OmniSwitch 6560	OS6560-P24Z8	ARM Cortex-A9	Multi-GigE fixed chassis in 1RU size. Includes 8 RJ-45 100/1G/2.5G BaseT HPoE, 16 RJ-45 10/100/1G BaseT PoE and 2xSFP+ (1G/10G) ports.
	OS6560-P24Z24	ARM Cortex-A9	Multi-GigE fixed chassis in 1RU size. Includes 24 RJ-45 100/1G/2.5G BaseT HPoE, 4xSFP+ (1G/10G) and 2x20G stacking ports.
	OS6560-P48Z16	ARM Cortex-A9	Multi-GigE fixed chassis in 1RU size. Includes 16 RJ-45 100/1G/2.5G BaseT HPoE, 32 RJ-45 10/100/1G BaseT PoE, 4xSFP+(1G/10G) and 2x20G stacking ports.
	OS6560-24Z8	ARM Cortex-A9	Multi-GigE fixed chassis in 1RU size. Includes 8 RJ-45 100/1G/2.5G BaseT, 16 RJ-45 10/100/1G BaseT and 2xSFP+ (1G/10G) ports.
	OS6560-24Z24	ARM Cortex-A9	Multi-GigE fixed chassis in 1RU size. Includes 24 RJ-45 100/1G/2.5G BaseT, 4xSFP+ (1G/10G) and 2x20G stacking ports.
	OS6560-24X4	ARM Cortex-A9	Gigabit fixed chassis in 1RU size. Includes 24 RJ-45 10/100/1G BaseT, 2xSFP(1G) and 4xSFP+ (1G/10G) uplink/stacking ports.
	OS6560-P24X4	ARM Cortex-A9	Gigabit fixed chassis in 1RU size. Includes 24 RJ-45 10/100/1G BaseT PoE+, 2xSFP(1G) and 4xSFP+ (1G/10G) uplink/stacking ports.
	OS6560-48X4	ARM Cortex-A9	Gigabit fixed chassis in 1RU size. Includes 48 RJ-45 10/100/1G BaseT, 2xSFP(1G) and 4xSFP+ (1G/10G) uplink/stacking ports.
	OS6560-P48X4	ARM Cortex-A9	Gigabit fixed chassis in 1RU size. Includes 48 RJ-45 10/100/1G BaseT PoE+, 2xSFP(1G) and 4xSFP+ (1G/10G) uplink/stacking ports.
	OS6560-X10	ARM Cortex-A9	10GigE fixed chassis 8 SFP+ 10GigE, 2 QSFP+ (20G) stacking ports.
OmniSwitch 6860	OS6860-24	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.

Family Series	Hardware ID	Processor	Description
	OS6860-P24	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.
	OS6860-48	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.
	OS6860-P48	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.
	OS6860E-24	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
	OS6860E-P24	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
	OS6860E-48	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
	OS6860E-P48	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
	OS6860E-U28	ARM Cortex-A9	Fixed-configuration chassis in a 1U form factor with 28 ports supporting 1000Base-X and 100Base-FX, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
	OS6860E-P24Z8	ARM Cortex-A9	GigE L3 Fixed-configuration chassis. Includes 16 10/100/1000 Base-T PoE+ ports, eight 2.5G 802.3bz HPoE(75W) ports, four fixed SFP+ (1G/10G) ports and two Virtual Chassis link ports.
OmniSwitch 6865	OS6865-P16X	ARM Cortex-A9	Hardened Stackable Gigabit Ethernet L3 fixed configuration switches for harsh temperature, physical and electrical conditions. It has twelve RJ-45 10/100/1000 Base-T ports with eight ports PoE+ and four ports 60W PoE capable, two 1000 Base-X SFP ports and two fixed SFP+ (1G/10G) ports. It provides Shortest Path Bridging MAC (SPBM), advanced routing and QoS capabilities. It also provides IEEE 1588v2 PTP capability on all ports.
	OS6865-U12X	ARM Cortex-A9	Hardened GigE L3 fixed configuration fan-less chassis. Includes four 100/1000 Base-X SFP ports, two 1000 Base-X SFP Ports, four 10/100/1000 Base-T 75W HPoE ports, two SFP+ (1G/10G) ports, RS-232

Family Series	Hardware ID	Processor	Description
	OS6865-U28X	ARM Cortex-A9	Hardened GigE L3 fixed configuration fan-less chassis Includes 20 100/1000 Base-X SFP ports, four SFP+ (1G/10G) ports, four 10/100/1000 Base-T 75W HPoE ports, RS-232 Console (RJ45), USB, and two 20G VFL QSFP+ ports.
OmniSwitch 6900	OS6900-X20	NXP MPC8572	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with twenty SFP+ ports, one optional module slot.
	OS6900-X40	NXP MPC8572	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with forty SFP+ ports, two optional module slots.
	OS6900-T20	NXP QorIQ P2040	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with twenty 10GBase-T ports, auto-negotiable 100-BaseT, 1/10 GigE one optional module slot.
	OS6900-T40	NXP QorIQ P2040	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with forty 10GBase-T ports, auto-negotiable 100-BaseT, 1/10 GigE two optional module slots.
	OS6900-X72	NXP QorIQ P2040	10Gigabit/40Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with forty-eight 1/10G SFP+ ports and six 40G QSFP+ ports. QSFP+ ports operate as single 40GE port or Quad-10GE. Console and Ethernet management ports are RJ45.
	OS6900-Q32	NXP QorIQ P2040	40 Gb Ethernet L3 fixed configuration chassis in a 1U form factor with thirty-two QSFP+ ports. Ports operate as single 40GigE port or Quad-10GigE.
	OS6900-V72	Intel Atom C2538	48 10/25 GigE SFP28 ports and six QSFP28 ports that operate at 100 GigE or 4x25 GigE or 40 GigE or 4x10 GigE. Maximum 25G port density is 72 ports.
	OS6900-C32	Intel Atom C2538	32 fixed QSFP28 ports in the front panel. The ports can operate at 100 GigE or 40 GigE. They can also operate as 4x25 GigE or 4x10 GigE using splitter cables. Maximum 25G port density is 128 ports.
OmniSwitch 9900	OmniSwitch 9907 Chassis	Not applicable	The OmniSwitch 9900 chassis offers six slots for high-capacity 1/10/40-Gigabit Ethernet Network Interface (NI) modules. Additional slots are used for primary and redundant Chassis Management Modules (CMMs), Chassis Fabric Modules (CFMs), fan trays and power supplies. At least one CMM, an additional CMM or CFM , and one NI are required to assembly an operational network switch.
	OS9907-CFM	Not applicable	This CFM provides expanded switching fabric for the chassis, which increases switching throughput and provides redundancy.
	OS99-CMM	Intel Atom C2518	This CMM includes a processor module, a fabric module, two 40G QSFP ports, and AOS software with advanced IP routing SW (IPv4/IPv6).

Family Series	Hardware ID	Processor	Description
	OS99-XNI-48	Intel Atom C2338[2]	This 10 Gigabit network interface (XNI) card offers forty-eight wirerate 10GBase-T ports.
	OS99-XNI-U48	Intel Atom C2338	This XNI card offers forty-eight wirerate unpopulated SFP+ ports with 1/10 Gbps connections.
	OS99-GNI-48	Intel Atom C2338	This Gigabit network interface (GNI) card offers forty-eight wirerate RJ-45 10/100/1000Base-T ports.
	OS99-GNI-P48	Intel Atom C2338	This GNI card offers forty-eight wirerate RJ-45 10/100/1000Base-T ports with PoE.
	OS99-CNI-U8	Intel Atom C2338	This network interface card offers 8 unpopulated wire rate QSFP28 100GE ports.
	OS99-XNI-P24Z8	Intel Atom C2338	This XNI card offers 16 10G-Base-T ports and 8 1/2.5/5/10G Base-T ports.
	OS99-XNI-P48Z16	Intel Atom C2338	This XNI card offers 32 RJ-45 10G Base-T and 16 RJ-45 1/2.5/5/10G Base-T wire rate PoE ports.
	OS99-XNI-U12Q	Intel Atom C2338	This XNI card offers 12 unpopulated wire rate SFP+ 1/10 GbE ports.
	OS99-XNI-U24	Intel Atom C2338	This XNI card offers 24 unpopulated wire rate SFP+ 1/10 GbE ports.
	OS99-XNI-U48	Intel Atom C2338	This XNI card offers 48 1/10G wire rate unpopulated SFP+ ports.
	OS99-XNI-UP24Q2	Intel Atom C2338	This XNI card offers 12 unpopulated SFP+ 1/10 GbE ports and 12 10G-Base-T ports.

Table 2: TOE Hardware Components

1.5.2.1.2 TOE Guidance

The following documentation comprises the TOE guidance and is available on the Alcatel-Lucent Enterprise Service and Support website.

- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.6.R11 [AOS8-CCGUIDE]
- AOS Release 8.3.1 Release Notes [AOS8-RN]
- OmniSwitch AOS Release 8 Switch Management Guide [AOS8-SM]
- OmniSwitch AOS Release 8 CLI Reference Guide [AOS8-CLI]
- OmniSwitch AOS Release 8 Network Configuration Guide [AOS8-NC]
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide [AOS8-ARC]
- OmniSwitch AOS Release 8 Transceivers Guide [AOS8-TCV]
- OmniSwitch AOS Release 8 Data Center Switching Guide [AOS8-DCS]

[2] No cryptographic functionality runs in the Intel Atom C2338 processor, as it is only used for Network Interface (NI) cards.

- OmniSwitch 6465 Hardware Users Guide [OS6465-HWUG]
- OmniSwitch 6560 Hardware Users Guide [OS6560-HWUG]
- OmniSwitch 6860 Hardware Users Guide [OS6860-HWUG]
- OmniSwitch 6865 Hardware Users Guide [OS6865-HWUG]
- OmniSwitch 6900 Hardware Users Guide [OS6900-HWUG]
- OmniSwitch 9900 Hardware Users Guide [OS9900-HWUG]

1.5.2.1.3 Delivery of the TOE

Alcatel-Lucent Enterprise orders for the Common Criteria evaluated TOE are delivered using reputable couriers for shipping. The TOE is typically located in a physically secure environment, accessible only by authorized personnel.

Hardware is packaged in electrostatic discharge (ESD) bags and sealed with an ESD warning label. It is then boxed in the factory using sealing tape with the “Alcatel Lucent Enterprise” banner and the company logo. The corrugated box has a label containing the serial number of the unit inside.

The Administrator has to follow a documented procedure to verify the TOE received. The Hardware Guide appropriate to the specific TOE addresses unpacking the TOE and provides a list of expected package contents. The customer needs to ensure that:

- the shipping label exactly identifies the correct customer name and address as well as the TOE.
- the TOE is packaged in ESD bags and sealed with an ESD warning label.
- the TOE is boxed and has factory sealing tape with “Alcatel-Lucent Enterprise” and the logo. This tape seal would be broken or missing if the box was opened during transit.

If the customer identifies a problem during the inspection, he or she must immediately contact the supplier (i.e. Alcatel Lucent Enterprise) , providing the order number, tracking number, and a description of the identified problem.

The TOE is shipped with the evaluated AOS firmware installed. The version can be confirmed by the administrator by entering the CLI command `show microcode loaded`. The evaluated AOS firmware can be also obtained from the Alcatel-Lucent Enterprise Service and Support website.

The TOE guidance can be downloaded from the Alcatel-Lucent Enterprise Service and Support website. Document part and revision numbers corresponding to the CC evaluated version are printed on the title page, with the part number in the header of every page.

As mentioned above, the Alcatel-Lucent Enterprise Service and Support website (https://businessportal2.alcatellucent.com) enables the secure download of all applicable documentation, the Common Criteria evaluated AOS firmware and any optional purchased software or upgrades. In order to access this website, the user must have a support contract in place.

1.5.2.2 Logical

This section contains the product features and denotes which are in the TOE.

1.5.2.2.1 Audit

The TOE generates audit records. The audit records can be displayed on the serial console as they are generated in a scrolling format.

The TOE writes audit records to a text file stored in the systems flash memory for permanent storage. These entries are tagged with the AOS Application ID that created them. The TOE also provides the ability to send the audit records to an external syslog server using a secure channel.

The TOE provides to security administrators the ability to modify the maximum size allowed for the audit files. Once the files are full the oldest entries are overwritten.

1.5.2.2.2 Administrator Identification and Authentication

The TOE requires identification and authentication of administrators of the TOE prior to access any of the management functionality in all possible scenarios, which are as follows:

- TOE administrators accessing (either locally or remotely) the Command Line Interface (CLI) via a serial console or a Secure Shell (SSH) session.
- TOE administrators accessing TOE storage using SFTP via an SSH session.
- A SNMP Management Station accessing the TOE through the SNMP management interface.

The TOE displays to the administrator a configurable banner after the administrator successfully logs onto the TOE (either serial console, SSH, or SFTP). The TOE also provides the ability to lock the administrator after a configurable number of unsuccessful attempts, and terminate the logon session after a configurable period of inactivity.

The TOE provides administrator configurable password settings to enforce password complexity when a password is created or modified.

The TOE provides support for the following Identification and Authentication mechanisms:

- Identification and Authentication made by the TOE using credentials stored in the local file system;
- Identification and Authentication made by the TOE using credentials stored in a Lightweight Directory Access Protocol (LDAP) server, which is part of the operational environment; or
- Identification and Authentication made by an external authentication server, which is part of the operational environment.

The only external authentication server supported by the TOE for administrator authentication in the evaluated configuration is Remote Authentication Dial In User Service (RADIUS).

Communications with RADIUS servers, LDAP servers and SNMP Management stations are protected with the Transport Layer Security (TLS) protocol. Communication with SSH and SFTP clients are protected with the Secure Shell (SSH) protocol.

1.5.2.2.3 End user and device authentication

Authentication of end users or devices is used to dynamically assign network devices to a VLAN domain and enforcing the VLAN and Traffic Filtering policies. Authentication is performed by verifying the credentials of the end user or the device. The TOE supports two types of authentication: Media Access Control (MAC) based authentication (for devices) and IEEE 802.1X authentication (for end users). The sections below describe the supported mechanisms.

1.5.2.2.3.1 MAC-based authentication

This authentication mechanism verifies the identity of the device based on its MAC address. MAC-based authentication is performed using a RADIUS server in the operational environment. Communication between the TOE and the RADIUS server is protected by the TLS protocol.

1.5.2.2.3.2 IEEE 802.1X authentication

Devices attached to a physical port are authenticated by the TOE through IEEE 802.1X using the Extensible Authentication Protocol (EAP). This feature provides port-based Network Access Control for external devices using end user credentials and is the recommended solution to provide the highest level of security for end user authentication.

There are three components for IEEE 802.1X as follows:

- *The Supplicant*: this is the device residing in the TOE operating environment that supports the 802.1x protocol and is connected to the TOE. The device may be connected directly to the TOE or via a point-to-point LAN segment. Typically the supplicant is a Personal Computer (PC) or laptop. A client is installed on the supplicant to support 802.1X authentication.
- *The Authenticator Port Access Entity (PAE)*: this entity requires authentication from the supplicant. The authenticator is connected to the supplicant directly or via a point-to-point LAN segment. The TOE acts as the authenticator PAE.
- *The Authentication Server*: this component resides in the TOE operating environment and provides the authentication service and verifies credentials (username, password, challenge, etc.) of the supplicant. The credentials to be verified can be the credentials of the device.

IEEE 802.1X authentication is performed using a RADIUS server in the operational environment. Communication between the TOE and the RADIUS server is protected through the TLS protocol.

Figure 3 shows a depiction of IEEE 802.1X end user authentication provided by the TOE.

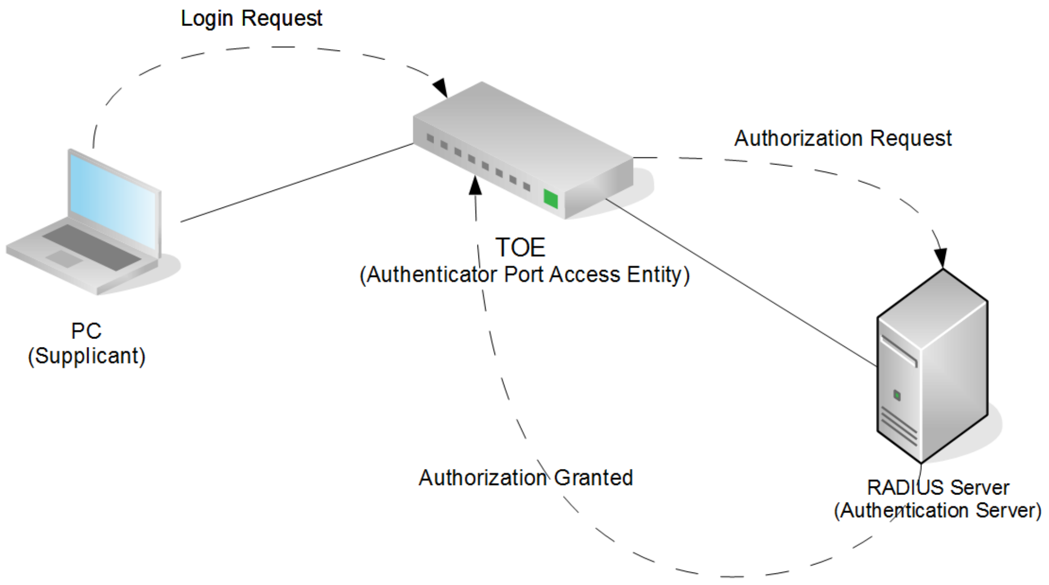

Figure 3: IEEE 802.1X end user authentication

1.5.2.2.4 Management of the TOE

The TOE provides a Command-Line Interface (CLI) for security management. TOE administrators connect to the TOE via either a serial console or a remote session using Secure Shell (SSHv2). In either case, administrators are required to identify and authenticate against the TOE before getting access to the CLI.

The TOE provides an SNMPv3 management interface for security management functionality. An SNMP Management Station authenticates to the TOE and can send request commands to get and set configuration information.

The TOE also provides a Flash file system used for storing configuration files/directories. TOE administrators connect to the TOE via the Secure File Transfer Protocol (SFTP), providing their credentials to identify and authenticate against the TOE before any action.

The TOE provides the administrator the ability to create, modify & delete policies that meditate traffic flow as implemented by the Traffic Filter SFP or Virtual Local Area Network (VLAN) SFP.

1.5.2.2.5 Cryptographic support

The TOE requires cryptography for supporting the following functionality.

- Establishment of secure channels using the SSHv2, TLSv1.1 and TLSv1.2 protocols.
- X.509 certificate generation and validation.
- Storage of passwords.
- Self-tests of the cryptographic algorithms.
- Verification of the integrity of the TOE firmware.

The TOE provides cryptographic support using the OpenSSL and OpenSSH software packages, which are bundled in the TOE.

1.5.2.2.6 Traffic Mediation

The TOE provides filtering of network traffic through two mechanisms: Virtual Local Area Network (VLAN) configuration and traffic filtering based on Access Control Lists (ACLs).

1.5.2.2.6.1 VLANs

The TOE enforces VLAN separation by allowing IP packets to be sent only within the VLAN that matches the VLAN id assigned to the packet. VLAN traffic is not available in other VLANs, unless there is an IP interface between VLANs (IP forwarding).

A VLAN can be assigned to a physical port of the TOE (by default, VLAN 1 is assigned to all physical ports). When a packet is received from that port, the TOE inserts the VLAN id into the packet. The packet is then bridged to other ports that are assigned to the same VLAN id. See Figure 4 for an example.

The TOE also supports VLAN identification through the VLAN tagging mechanism conformant to IEEE 802.1Q. In this deployment, the TOE extracts the VLAN tag included in the packet header to identify the VLAN ID. If the egress port of the TOE is configured for the same tagged VLAN, the TOE re-inserts the VLAN tag and forwards the packet. This method allows the TOE to bridge traffic for multiple VLANs over one physical port connection; while one physical port can be assigned to one untagged VLAN (the default VLAN if the incoming IP packet does not include a IEEE 802.1Q tag), several tagged VLANs can be assigned to a physical port.

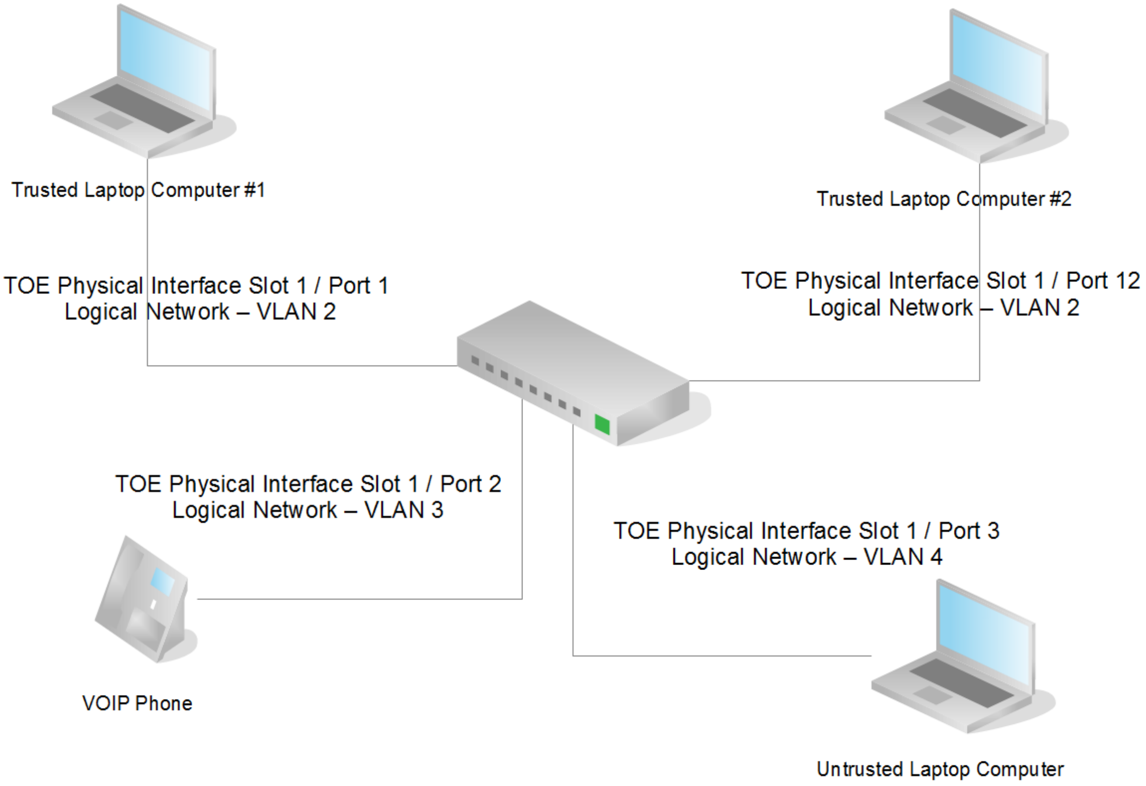
Trusted Laptop Computer #1
Trusted Laptop Computer #2
TOE Physical Interface Slot 1 / Port 1
Logical Network – VLAN 2
TOE Physical Interface Slot 1 / Port 12
Logical Network – VLAN 2
TOE Physical Interface Slot 1 / Port 2
Logical Network – VLAN 3
TOE Physical Interface Slot 1 / Port 3
Logical Network – VLAN 4
VOIP Phone
Untrusted Laptop Computer

Figure 4: Static VLAN port configuration

If a device needs to communicate with another device that belongs to a different VLAN, the TOE mediates the flow of information between the VLANs. As depicted in Figure 5 below, Layer-3 routing is necessary to transmit traffic between the VLANs. A VLAN is available for routing if an IP interface has been configured for forwarding on that VLAN. Therefore, workstations connected to ports on VLAN 1 can communicate with ports on VLAN 3.

If a VLAN does not have a router interface configured, the ports associated with the VLAN are isolated from other VLANs.

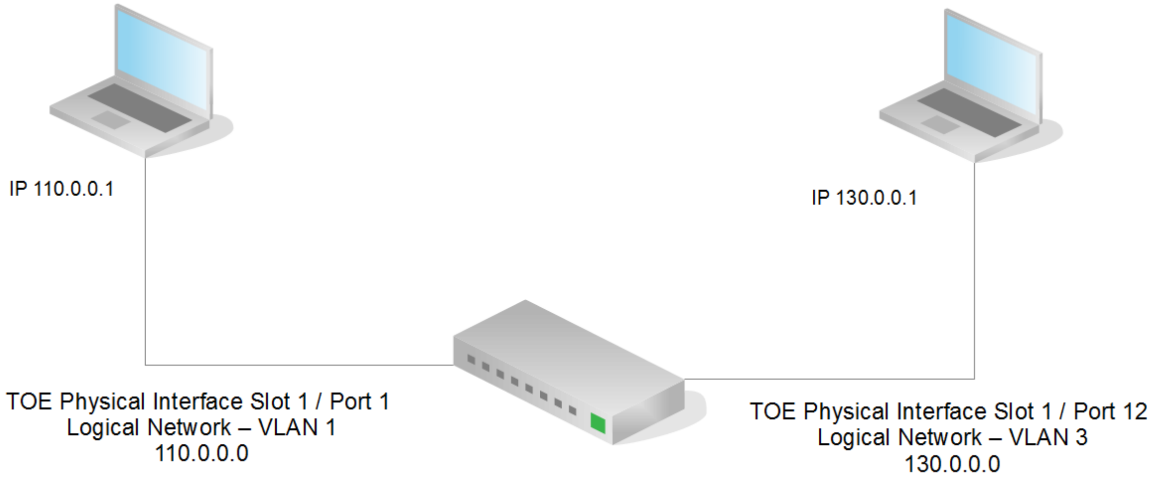

Figure 5: IP forwarding

The TOE also allows dynamic association of incoming traffic to a VLAN on non-fixed ports, based on the results of the end user or the device authentication (failure or success of MAC-based and/or IEEE 802.1X mechanisms), the application of classification rules, the association with a Universal Network Profile (UNP) or default VLAN IDs assigned to the port in case no matching rule is found.

1.5.2.2.6.2 Traffic Filtering

Traffic Filtering is implemented using ACLs to moderate traffic flow between networks. When traffic arrives on the TOE, and once a logical network is assigned to the IP packet, the TOE checks its policy database to attempt to match Layer-2 (bridging) or Layer-3 / 4 (routing) information in the packet header to a filtering policy rule. If a match is found, it applies the permit or deny operation assigned to the rule. The default is to allow the traffic (this default can be changed by the security administrator).

The TOE allows the configuration of the traffic filtering policies using a combination of attributes at Layer-2 (e.g. MAC address, source VLAN, physical slot/port), Layer-3 (e.g. source IP address, destination IP address, IP protocol) or Layer-4 (e.g. source, destination TCP/UDP port). The TOE can also perform limited filtering of IPv6 traffic, and can filter multicast traffic via the Internet Group Management Protocol (IGMP). Figure 6 below depicts examples of traffic filtering.

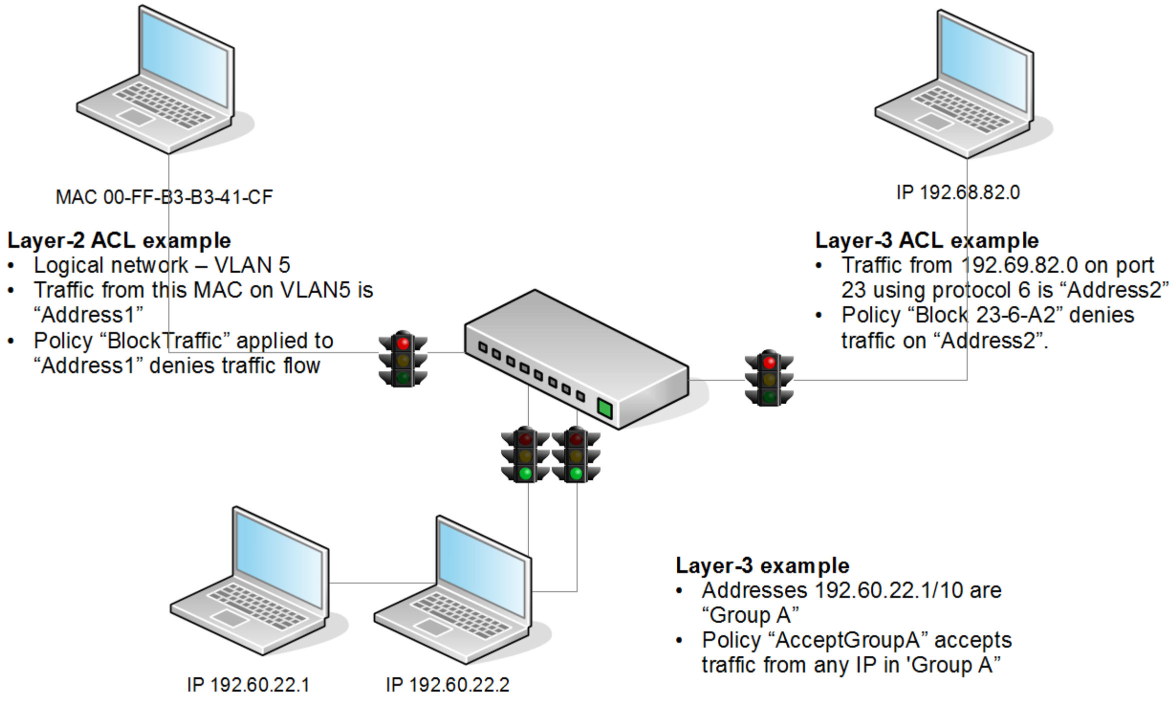
MAC 00-FF-B3-B3-41-CF
Layer-2 ACL example
• Logical network – VLAN 5
• Traffic from this MAC on VLAN5 is "Address1"
• Policy "BlockTraffic" applied to "Address1" denies traffic flow
IP 192.68.82.0
Layer-3 ACL example
• Traffic from 192.69.82.0 on port 23 using protocol 6 is "Address2"
• Policy "Block 23-6-A2" denies traffic on "Address2".
Layer-3 example
• Addresses 192.60.22.1/10 are "Group A"
• Policy "AcceptGroupA" accepts traffic from any IP in 'Group A"
IP 192.60.22.1
IP 192.60.22.2

Figure 6: Traffic filtering

1.5.2.2.7 Protection of the TSF

The TOE protects itself by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator. The TOE uses the filesystem access control to protect access to sensible data like cryptographic keys and credentials.

The TOE ensures that manual updates of the TOE firmware are done using trusted updates by verifying the integrity of the new version of the TOE firmware.

The TOE also implements self-tests to ensure the correct operation of cryptographic services.

The TOE also provides a reliable date and time that is used for audit record timestamps, certificate verification and session timing.

1.5.2.2.8 Trusted path/channels

The TOE provides the following secure channels to ensure the integrity and confidentiality of the information exchanged between the TOE and external IT entities in the operational environment.

- Transport Layer Security (TLS) versions 1.1 and 1.2 are used to protect communication with authentication servers (RADIUS), LDAP servers, SNMP Management stations, and audit servers (syslog).
- Secure Shell version 2 (SSHv2) is used to protect communication with SSH and SFTP clients and servers.

1.5.2.3 Non-Security Relevant TOE Features

The following table identifies other AOS features that are not security relevant and their usage does not impact the overall security of the product.

Feature	Description
LDAP Policy Server	LDAP Policy Server features are used to manage LDAP Policies. LDAP policies are QoS policies that are created via the PolicyView application and stored on an external LDAP server. The Policy Manager in the TOE downloads these policies and keeps track of them. These policies cannot be modified directly on the TOE. Since policies may only be modified via their originating source, LDAP policies must be modified through PolicyView and downloaded again to the TOE.
Load balancing	Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (e.g., web servers). SLB uses a Virtual IP (VIP) address to treat a group of physical servers, each with a unique IP address, as one large virtual server. The TOE will process requests by clients addressed to the VIP of the SLB cluster and send them to the physical servers. This process is totally transparent to the client.
Distance Vector Multicast Routing Protocol (DVMRP) / Protocol-Independent Multicast (PIM)	IP Multicast Routing Protocols
Spanning Tree	The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel STP implementation distributes the STP load between the primary management module and the network interface modules. In the case of a stack of switches, the STP load is distributed between the primary management switch and other switches in the stack.
Link Aggregation	Link aggregation allows you to combine two, four, or eight physical connections into large virtual connections known as link aggregation groups. You can configure VLANs, QoS conditions, 802.1Q framing, and other networking features on link aggregation groups because the TOE treats these virtual links just like physical links.

Table 3: TOE functionality excluded from the TSF

1.5.2.4 Excluded TOE Features

The following features interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration.

Virtual Chassis mode

This feature allows a group of switches to operate as a single bridge and router. The TOE must always operate in Standalone mode.

Captive Portal

This feature allows web-based authentication of end-users.

Terminal Access Controller Access-Control System Plus (TACACS+)
Authentication using an external TACACS+ server is not allowed in the CC evaluated configuration.

Port Mobility Rules

Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic.

This feature is superseded by User network profiles and has been kept in the product for backwards compatibility reasons.

FTP access to the TOE
FTP traffic is not secured so the FTP service must be disabled for security reasons.

Telnet access to the TOE
Telnet traffic is not secured so the Telnet service must be disabled for security reasons.

Webview
This web-based interface used for management must be disabled.

Simple Network Management Protocol (SNMP)
SNMP versions 1 and 2 must be disabled in the CC evaluated configuration. Only SNMP version 3 using TSM is allowed (i.e. protected by a secure channel using the TLS protocol).

Hypertext Transfer Protocol (HTTP)
HTTP and HTTPs must be disabled in the CC evaluated configuration.

Cryptographic algorithms
The MD5 algorithm cannot be used.

Network Time Protocol (NTP)
The use of NTP to synchronize the time with an external time source must be disabled in the CC evaluated configuration.

IPSec
IPSec must be disabled in the CC evaluated configuration.

1.5.2.5 Operational Environment

This section describes requirements on the environment in which the TOE is operated. The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only security administrators are to have access to connect to the serial console, or gain physical access to the hardware storing log data. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

- If the TOE is part of a network where network addresses are assigned dynamically, a Dynamic Host Configuration Protocol (DHCP) server is required in the operational environment. Communication between the TOE and the DHCP server must be reliable and protected from loss of integrity by physical or logical means.
- Versions 1.1 and 1.2 of the TLS protocol are the only versions allowed in the evaluated configuration. Usage of other protocol versions usually supported in SSL and TLS (SSLv2.0, SSLv3.0 or TLSv1.0) are prohibited.
- If the TOE is configured to use a RADIUS authentication server, or an LDAP server for credential storage, the TOE is dependent upon this external server in the operational environment for authentication.

- If the TOE is configured to use an LDAP server for credential storage, then a TLSv1.1 or TLSv1.2 capable LDAP server is required in the operational environment.
- If the TOE is configured to use a RADIUS external server for credential storage, then a TLSv1.1 or TLSv1.2 capable RADIUS server is required in the operational environment.
- If the TOE is configured to perform IEEE 802.1X authentication, then the TOE is dependent upon an IEEE 802.1X client to be on the end user device attached to the LAN port in the TOE operating environment. This client is built into most standard current operating systems. In addition, if 802.1X is enabled, the TOE is dependent upon a RADIUS authentication server in the TOE operational environment.
- If the TOE is configured to use SNMP, only SNMPv3 can be used and protected with the Transport Security Model (TSM) ("snmp security tsm enable" setting); In addition, a TLSv1.1 or TLSv1.2 capable SNMP Network Management Station is required in the operational environment.
- If the TOE is configured to send logging output files (syslog files) to a remote IP address, a TLSv1.1 or TLSv1.2 capable syslog server is required in the operational environment.
- If the domain name is used as an identifier in the Subject Alternative Names (SAN) of external servers' certificates (LDAP, SNMP, Syslog, Radius), then the Domain Name Server (DNS) must be configured to support reverse DNS so server certificates can be validated during the TLS session establishment.
- A serial console connected to the appliance must be available for installation and initial configuration. Once installation and configuration is completed, access to the TOE can be performed via the serial console as well as a remote console.
- If remote console is used, the Operational Environment must include an SSHv2 client.
- File transfers between the TOE and external servers, when the TOE is acting either as a client or a server, must be only performed using SFTP. FTP and Trivial File Transfer Protocol (TFTP) are forbidden. In this case, the Operational Environment must include an SFTP client or server.

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL2, augmented by ALC_FLR.2.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

The **assets** to be protected by the TOE are as follows.

- Communications with the TOE: for administering the TOE (administration traffic), for sending and receiving authentication information sent to external servers (authentication traffic), and for sending audit records to an external audit server (audit traffic).
- The current version of the TOE and trusted updates to its firmware.
- TSF data stored by the TOE (e.g. user credentials, digital certificates).

The **threat agents** having an interest in manipulating the data model can be categorized as either:

- Unauthorized individuals (“attackers”) which are unknown to the TOE and its runtime environment.
- Authorized users of the TOE (i.e., administrators) who try to manipulate data that they are not authorized to access.

Threat agents originate from a well managed user community within an organizations internal network. Hence, only inadvertent or casual attempts to breach system security are expected from this community.

TOE administrators, including administrators of the TOE environment, are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Hence, only inadvertent attempts to manipulate the safe operation of the TOE are expected from this community.

3.1.1 Threats countered by the TOE

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints (e.g. a shared password that is guessable or transported as plaintext). The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker’s credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.

T.INFORMATION_FLOW_POLICY_VIOLATION

An unauthorized individual or an IT external entity may send messages through the TOE, which violates the permissible information flow rules enforced by the TOE.

3.2 Assumptions

3.2.1 Intended usage of the TOE

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

3.2.2 Environment of use of the TOE

3.2.2.1 Physical

A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

3.2.2.2 Personnel

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE’s trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

The Administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.2.2.3 Connectivity

A.SERVICES_RELIABLE

All network services in the Operational Environment provide reliable information and responses to the TOE. In case the TSF does not provide a secure channel for the network service, it is assumed that the Operational Environment protects the communication between the network service and the TOE from loss of integrity, either by physical or logical means.

3.3 Organizational Security Policies

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

P.SELF_TESTS

The TOE shall ensure the reliability of the cryptographic functionality used in the TOE security functionality by performing self-tests at start-up and during operation.

4 Security Objectives

4.1 Objectives for the TOE

O.ADMIN_ACCESS

The TOE must ensure that only identified and authenticated users gain access to administrative functions and protected resources.

O.ADMIN_SESSION

The TOE must protect interactive administrator's sessions by allowing the termination of sessions by an administrator, and forcing the termination of a session after a specified period of inactivity.

O.CRYPTOGRAPHY

The TOE must use standardized cryptographic algorithms, which must provide sufficient strength through the use of appropriate key sizes and modes. Key generation algorithms must use a standardized Deterministic Random Bit Generator (DRBG) seeded with an amount of entropy equal or greater of the strength of the cryptographic keys generated.

O.COMMUNICATION_CHANNELS

The TOE must protect critical network traffic from disclosure and modification using standardized secure tunneling protocols. These protocols must use strong cryptographic algorithms and authentication methods for each endpoint. Critical network traffic includes transfer of TSF data to and from the TOE, administrators performing security management activities, and communication with external IT entities used by the TOE to support the TSF (e.g. an external authentication server).

O.TRUSTED_UPDATES

The TOE must verify the authenticity of software or firmware updates before being installed through one or more authentication methods using strong cryptographic algorithms.

O.AUDIT

The TOE must record security relevant actions of users on the TOE. The information recorded in these security events must be in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features.

O.TSF_DATA_PROTECTION

The TOE must protect the network device software, firmware, and TSF data (administrator credentials, credentials used for secure channels, etc.) from unauthorized disclosure and modification.

O.STRONG_PASSWORDS

The TOE must enforce the use of a password policy for administrative credentials.

O.SELF_TESTS

The TOE must ensure the reliability of the cryptographic functionality used in the TOE security functionality by performing self-tests at start-up and during operation.

O.ACCESS_BANNER

The TSF must display an initial banner before users log into the TOE. The initial banner must contain restrictions of use, legal agreements, or any other appropriate information to which users make consent by accessing the TOE.

O.MEDIATE

The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information in the TOE from a previous information flow is not transmitted in any way.

4.2 Objectives for the Operational Environment

OE.PHYSICAL

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

OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.TRUSTED_ADMIN

Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE’s trust store in case such certificate can no longer be trusted.

OE.UPDATES

The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.ADMIN_CREDENTIALS_SECURE

The Administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.RESIDUAL_INFORMATION

The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

OE.SERVICES_RELIABLE

All network services in the Operational Environment shall provide reliable information and responses to the TOE. If the TSF does not provide a secure channel for the network service, communication between the network service and the TOE must be protected from loss of integrity, either by physical or logical means, by the Operational Environment.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	**Threats / OSPs**
O.ADMIN_ACCESS	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
O.ADMIN_SESSION	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
O.CRYPTOGRAPHY	T.WEAK_CRYPTOGRAPHY
O.COMMUNICATION_CHANNELS	T.UNTRUSTED_COMMUNICATION_CHANNELS T.WEAK_AUTHENTICATION_ENDPOINTS
O.TRUSTED_UPDATES	T.UPDATE_COMPROMISE
O.AUDIT	T.UNDETECTED_ACTIVITY
O.TSF_DATA_PROTECTION	T.SECURITY_FUNCTIONALITY_COMPROMISE
O.STRONG_PASSWORDS	T.PASSWORD_CRACKING
O.SELF_TESTS	P.SELF_TESTS
O.ACCESS_BANNER	P.ACCESS_BANNER
O.MEDIATE	T.INFORMATION_FLOW_POLICY_VIOLATION

Table 4: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	**Assumptions / Threats / OSPs**
OE.PHYSICAL	A.PHYSICAL_PROTECTION
OE.NO_GENERAL_PURPOSE	A.LIMITED_FUNCTIONALITY
OE.TRUSTED_ADMIN	A.TRUSTED_ADMINISTRATOR
OE.UPDATES	A.REGULAR_UPDATES
OE.ADMIN_CREDENTIALS_SECURE	A.ADMIN_CREDENTIALS_SECURE
OE.RESIDUAL_INFORMATION	A.RESIDUAL_INFORMATION

Objective	Assumptions / Threats / OSPs
OE.SERVICES_RELIABLE	A.SERVICES_RELIABLE

Table 5: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Threat	Rationale for security objectives
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	The threat of gaining administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session , or performing man-in-the-middle attacks is countered by O.ADMIN_ACCESS and O.ADMIN_SESSION.
T.WEAK_CRYPTOGRAPHY	The threat of exploiting weak cryptographic algorithms or performing a cryptographic exhaust against the key space, because of poorly chosen encryption algorithms, modes, or key sizes is countered by O.CRYPTOGRAPHY.
T.UNTRUSTED_COMMUNICATION_CHANNELS	The threat of losing confidentiality and integrity of the critical network traffic, and potentially a compromise of the network device itself because of not using standardized secure tunneling protocols is countered by O.COMMUNICATION_CHANNELS.
T.WEAK_AUTHENTICATION_ENDPOINTS	The threat of having critical network traffic exposed because of using protocols that use weak methods to authenticate the endpoints is countered by O.COMMUNICATION_CHANNELS.
T.UPDATE_COMPROMISE	The threat of using a compromised update of the software or firmware tampered by an attacker is countered by O.TRUSTED_UPDATES.
T.UNDETECTED_ACTIVITY	The threat of access, change, and/or modify the security functionality of the network device without administrator awareness is countered by O.AUDIT.
T.SECURITY_FUNCTIONALITY_COMPROMISE	The threat of compromising credentials and device data enabling continued access to the network device and its critical data is countered by O.TSF_DATA_PROTECTION.
T.PASSWORD_CRACKING	The threat of gaining administrative access to the device because of using weak administrative passwords is countered by O.STRONG_PASSWORDS.

Threat	Rationale for security objectives
T.INFORMATION_FLOW_POLICY_VIOLATION	O.MEDIATE assures that the TOE must control the flow of information and enforce the configured information flow policy rules for the TOE.

Table 6: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	Rationale for security objectives
A.LIMITED_FUNCTIONALITY	The assumption: • The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). is upheld by: • OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL_PROTECTION	The assumption: • The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. is upheld by: • OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
A.TRUSTED_ADMINISTRATOR	The assumption: • The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. is upheld by:

Assumption	Rationale for security objectives
	• OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
A.REGULAR_UPDATES	The assumption: • The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities. is upheld by: • OE.UPDATES: The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The assumption: • The Administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside. is upheld by: • OE.ADMIN_CREDENTIALS_SECURE: The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
A.RESIDUAL_INFORMATION	The assumption: • The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. is upheld by: • OE.RESIDUAL_INFORMATION: The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.SERVICES_RELIABLE	The assumption: • All network services in the Operational Environment provide reliable information and responses to the TOE. In case the TSF does not provide a secure channel for the network service, it is assumed that the Operational Environment protects the communication between the network service and the TOE from loss of integrity, either by physical or logical means. is upheld by:

Assumption	Rationale for security objectives
	• OE.SERVICES_RELIABLE: All network services provided in the Operational Environment and used by the TOE must be reliable and, in case the TSF does not provide a secure channel between the TOE and the network service, this communication must be protected by the Operational Environment.

Table 7: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.ACCESS_BANNER	The organizational security policy that requires an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE is enforced by O.ACCESS_BANNER.
P.SELF_TESTS	The organizational security policy that requires the execution of self-tests at start-up and during operation is enforced by O.SELF_TESTS.

Table 8: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

This section defines the newly defined components (also known as extended components) used to define the security requirements for this ST.

This Security Target uses the following extended components from the collaborative Protection Profile for Network Devices, version 2.1 ([NDcPPv2.1]☝):

- FAU_STG_EXT.1 Extended: Protected audit event storage
- FCS_RBG_EXT.1 Extended: Random bit generation
- FCS_SSHC_EXT.1 Extended: SSH Client Protocol
- FCS_SSHS_EXT.1 Extended: SSH Server Protocol
- FCS_TLSC_EXT.2 TLS Client Protocol with authentication
- FCS_TLSS_EXT.2 Extended: TLS Server Protocol with mutual authentication
- FIA_PMG_EXT.1 Extended: Password management
- FIA_UIA_EXT.1 Extended: Identification and authentication
- FIA_UAU_EXT.2 Extended: Password-based authentication mechanism
- FIA_X509_EXT.1/Rev X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication
- FIA_X509_EXT.3 Extended: X509 Certificate Requests
- FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- FPT_APW_EXT.1 Protection of Administrator Passwords
- FPT_TST_EXT.1 TSF testing
- FPT_TUD_EXT.1 Trusted Update
- FPT_STM_EXT.1 Reliable Time Stamps
- FTA_SSL_EXT.1 TSF-initiated Session Locking

Notice that this Security Target does not claim conformance to this Protection Profile; the use of the extended components mentioned above is to take advantage of extended components already defined of network devices.

6 Security Requirements

6.1 TOE Security Functional Requirements

The Security Functional Requirements (SFRs) have been defined based on components included in CC Part 2, the Extended Component Definition (ECD) section of this ST, and the collaborative Protection Profile for Network Devices Version 2.1 ([NDcPPv2.1]).

Notice that this ST does not claim conformance to this Protection Profile; instead this ST reuses all the applicable extended components defined in Appendix C of [NDcPPv2.1] . In addition, applicable SFRs defined in Chapter 6, Appendix A and Appendix B of the same document are also considered, however, this ST assumes that the SFRs are defined in CC Part 2, therefore all assignment, selection, refinement and iteration operations used in the Protection Profile are repeated here to meet CC Part 2 extended conformance.

The table below summarizes the SFRs for the TOE and the operations performed on the components according to CC part 1. Operations in the SFRs use the following convention:

- Iterations (Iter.) are identified by appending a suffix to the original SFR.
- Refinements (Ref.) added to the text are shown in *italic text*, deletions are shown as ~~strikethrough text~~.
- Assignments (Ass.) are shown in **bold text**.
- Selections (Sel.) are shown in **bold text**.

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
	FAU_STG.1 Protected audit trail storage		CC Part 2	No	No	No	Yes
	FAU_STG_EXT.1 Extended: Protected audit event storage		NDcPPv2.1	No	No	Yes	Yes
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation		CC Part 2	No	Yes	Yes	No
	FCS_CKM.2 Cryptographic Key Establishment		CC Part 2	No	Yes	Yes	No
	FCS_CKM.4 Cryptographic key destruction		CC Part 2	No	No	Yes	No
	FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_RBG_EXT.1 Extended: Random bit generation		NDcPPv2.1	No	No	Yes	Yes
	FCS_SSHC_EXT.1 Extended: SSH Client Protocol		NDcPPv2.1	No	No	Yes	Yes
	FCS_SSHS_EXT.1 Extended: SSH Server Protocol		NDcPPv2.1	No	No	Yes	Yes
	FCS_TLSC_EXT.2 TLS Client Protocol with authentication		NDcPPv2.1	No	No	No	Yes
	FCS_TLSS_EXT.2 Extended: TLS Server Protocol with mutual authentication		NDcPPv2.1	No	No	No	Yes
FDP - User data protection	FDP_IFC.1/TF Subset information flow control (Traffic Filter)	FDP_IFC.1	CC Part 2	Yes	No	Yes	No
	FDP_IFF.1/TF Simple security attributes (Traffic Filter)	FDP_IFF.1	CC Part 2	Yes	Yes	Yes	No
	FDP_IFC.1/VLAN Subset information flow control (VLAN)	FDP_IFC.1	CC Part 2	Yes	No	Yes	No
	FDP_IFF.1/VLAN Simple security attributes (VLAN)	FDP_IFF.1	CC Part 2	Yes	No	Yes	No
	FDP_RIP.1 Subset residual information protection		CC Part 2	No	No	Yes	Yes
FIA - Identification and authentication	FIA_AFL.1 Authentication Failure Management		CC Part 2	No	No	Yes	Yes
	FIA_UAU.7 Protected authentication feedback		CC Part 2	No	Yes	Yes	No
	FIA_PMG_EXT.1 Password management		NDcPPv2.1	No	No	Yes	Yes
	FIA_UIA_EXT.1 User Identification and authentication		NDcPPv2.1	No	No	No	Yes
	FIA_UAU_EXT.2 Password-based Authentication Mechanism		NDcPPv2.1	No	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FIA_X509_EXT.1/Rev X.509 Certificate Validation		NDcPPv2.1	No	No	No	Yes
	FIA_X509_EXT.2 X.509 Certificate Authentication		NDcPPv2.1	No	No	No	Yes
	FIA_X509_EXT.3 Extended: X509 Certificate Requests		NDcPPv2.1	No	No	No	Yes
	FIA_SOS.1 Verification of secrets		CC Part 2	No	No	Yes	No
	FIA_ATD.1 End user and device attribute definition		CC Part 2	No	Yes	Yes	No
	FIA_UAU.1 Timing of authentication of end users and devices		CC Part 2	No	Yes	Yes	No
	FIA_UAU.5 Multiple authentication mechanisms for end users and devices		CC Part 2	No	Yes	Yes	No
	FIA_UID.1 Timing of identification of end users and devices		CC Part 2	No	Yes	Yes	No
	FIA_USB.1 End user and device subject binding		CC Part 2	No	Yes	Yes	No
FMT - Security management	FMT_MOF.1/ManualUpdate Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1/CoreData Management of TSF data	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		CC Part 2	No	No	Yes	No
	FMT_SMR.2 Restrictions on security roles		CC Part 2	No	No	Yes	No
	FMT_MOF.1/Services Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MOF.1/Functions Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1/CryptoKeys Management of TSF data	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1 Management of common security attributes		CC Part 2	No	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FMT_MSA.3 Static attribute initialization		CC Part 2	No	No	Yes	Yes
FPT - Protection of the TSF	FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)		NDcPPv2.1	No	No	No	No
	FPT_APW_EXT.1 Protection of Administrator Passwords		NDcPPv2.1	No	No	No	No
	FPT_TST_EXT.1 TSF testing		NDcPPv2.1	No	No	Yes	Yes
	FPT_TUD_EXT.1 Trusted Update		NDcPPv2.1	No	No	No	Yes
	FPT_STM_EXT.1 Reliable Time Stamps		NDcPPv2.1	No	No	No	Yes
FTA - TOE access	FTA_SSL.3 TSF-initiated Termination		CC Part 2	No	Yes	Yes	No
	FTA_SSL.4 User-initiated Termination		CC Part 2	No	Yes	No	No
	FTA_TAB.1 Default TOE Access Banners		CC Part 2	No	Yes	No	No
	FTA_SSL_EXT.1 TSF-initiated Session Locking		NDcPPv2.1	No	No	No	Yes
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		CC Part 2	No	Yes	Yes	Yes
	FTP_TRP.1 Trusted Path		CC Part 2	No	Yes	Yes	Yes

Table 9: SFRs for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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

a) Start-up and shut-down of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **All administrative actions comprising:**

- **Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).**
- **Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).**

- **Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).**
- **Resetting passwords (name of related user account shall be logged).**
- **Starting and stopping services.**

d) **Specifically defined auditable events listed in Table 10.**

Application Note: *The term "services" refers to trusted path and trusted channel communications and administrator sessions.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **information specified in column three of Table 10**.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1).	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.
FAU_STG.1	None.	None.
FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_TLSC_EXT.2	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSS_EXT.2	Failure to establish a TLS Session.	Reason for failure.
FMT_MOF.1/Services	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_MOF.1/Functions	None.	None.
FDP_IFC.1/TF	None.	None.
FDP_IFF.1/TF	None.	None.
FDP_IFC.1/VLAN	None.	None.
FDP_IFF.1/VLAN	None.	None.
FDP_RIP.1	None.	None.
FIA_SOS.1	None.	None.
FIA_ATD.1	None.	None.
FIA_UAU.1	None.	None.
FIA_UAU.5	None.	None.
FIA_UID.1	None.	None.
FIA_USB.1	None.	None.
FMT_MSA.1	None.	None.
FMT_MSA.3	None.	None.

Table 10: Security Functional Requirements and Auditable Events

6.1.1.2 User identity association (FAU_GEN.2)

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

6.1.1.3 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

6.1.1.4 Extended: Protected audit event storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

a) **TOE shall consist of a single standalone component that stores audit data locally**.

FAU_STG_EXT.1.3 The TSF shall **overwrite previous audit records according to the following rule: overwrite the data present in the oldest audit file** when the local storage space for audit data is full.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate *asymmetric* cryptographic keys in accordance with a specified cryptographic key generation algorithm*:*

- **RSA schemes using cryptographic key sizes of 2048 bits and 3072 bits that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;**
- **ECC schemes using “NIST curves" P-256, P-384, P-521 that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;**
- **FFC schemes using Diffie-Hellman group 14 and Diffie-Hellman group 16 that meet the following: [RFC3526]☝, Section 3**

~~and specified cryptographic key sizes~~ ~~that meet the following:~~ .

6.1.2.2 Cryptographic Key Establishment (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall ~~distribute cryptographic keys~~ *perform cryptographic key establishment* in accordance with a specified cryptographic key ~~distribution~~ *establishment* method*:*

- **RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of [RFC8017]☝, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1";**
- **Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";**
- **Key establishment scheme using Diffie-Hellman group 14 and group 16 that meets the following: [RFC3526]☝, Section 3;**

~~that meets the following:~~ .

6.1.2.3 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- **For plaintext keys in volatile memory, the destruction shall be executed by a single direct overwrite consisting of zeroes**
- **For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that instructs a part of the TSF to destroy the abstraction that represents the key**

that meets the following: **No Standard** .

6.1.2.4 Cryptographic Operation (Data Encryption/Decryption) (FCS_COP.1/DataEncryption)

FCS_COP.1.1 / DataEncryption The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES used in CBC, CTR and GCM modes** and cryptographic key sizes **128 bits, 192 bits and 256 bits for AES in CBC mode, 128 bits and 256 bits for AES in GCM and CTR modes** that meet the following: **AES as specified in ISO 18033-3, CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772**.

Application Note: *This SFR defines the cryptographic functionality implemented in OpenSSL and the kernel crypto library in AOS 8.6.4.R11.*

6.1.2.5 Cryptographic Operation (Signature Generation and Verification) (FCS_COP.1/SigGen)

FCS_COP.1.1 / SigGen The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm

- **RSA Digital Signature Algorithm and cryptographic key sizes (modulus) 2048 bits and 3072 bits**
- **Elliptic Curve Digital Signature Algorithm and cryptographic key sizes 256 bits, 384 bits and 512 bits**

~~and cryptographic key sizes~~ that meet the following:

- **For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3**
- **For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521; ISO/IEC 14888-3, Section 6.4**

.

6.1.2.6 Cryptographic Operation (Hash Algorithm) (FCS_COP.1/Hash)

FCS_COP.1.1 / Hash The TSF shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm **SHA-1, SHA-256, SHA-384, SHA-512** ~~and cryptographic key sizes~~ *and message digest sizes* **160, 256, 384, 512 bits** that meet the following: **ISO/IEC 10118-3:2004**.

Application Note: *This SFR defines the cryptographic functionality implemented in OpenSSL and the kernel crypto library in AOS 8.6.4.R11.*

6.1.2.7 Cryptographic Operation (Keyed Hash Algorithm) (FCS_COP.1/KeyedHash)

FCS_COP.1.1 / KeyedHash The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512** and cryptographic key sizes **256 bits** *and message digest sizes 160, 256, 384 and 512 bits* that meets the following: **ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”**.

Application Note: *This SFR defines the cryptographic functionality implemented in OpenSSL and the kernel crypto library in AOS 8.6.4.R11.*

6.1.2.8 Extended: Random bit generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using **Hash_DRBG (SHA-1, SHA-256, SHA-384, SHA-512), HMAC_DRBG (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512), CTR_DRBG (AES-256)**.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from **a single software-based noise source** with a minimum of **256 bits** of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.1.2.9 Extended: SSH Client Protocol (FCS_SSHC_EXT.1)

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) **4251, 4252, 4253, 4254, 4344, 5656, 6668, 8332**.

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in [RFC4252]☝: public key-based, **password-based**.

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in [RFC4253]☝, packets greater than **256K** bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: **aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com**.

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses **ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512** as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 The TSF shall ensure that **diffie-hellman-group14-sha1, ecdh-sha2-nistp256** and **diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and **no other methods** as described in [RFC4251]☝ section 4.1.

6.1.2.10 Extended: SSH Server Protocol (FCS_SSHS_EXT.1)

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) **4251, 4252, 4253, 4254, 4344, 5656, 6668, 8332**.

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in [RFC4252]☝: public key-based, **password-based**.

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in [RFC4253]☝, packets greater than **256K** bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: **aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com**.

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses **ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512** as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that **diffie-hellman-group14-sha1, ecdh-sha2-nistp256** and **diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

6.1.2.11 TLS Client Protocol with authentication (FCS_TLSC_EXT.2)

FCS_TLSC_EXT.2.1 The TSF shall implement **TLS 1.2 ([RFC5246]☝), TLS 1.1 ([RFC4346]☝)** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- **TLS_RSA_WITH_AES_128_CBC_SHA as defined in [RFC3268]**☝
- **TLS_RSA_WITH_AES_256_CBC_SHA as defined in [RFC3268]**☝
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in [RFC4492]**☝
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in [RFC4492]**☝
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in [RFC4492]**☝
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in [RFC4492]**☝
- **TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5246]**☝
- **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in [RFC5246]**☝
- **TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5288]**☝
- **TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5288]**☝
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5289]**☝
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in [RFC5289]**☝
- **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]**☝
- **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]**☝
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]**☝
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]**☝
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5289]**☝
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in [RFC5289]**☝

.

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifiers of the following types: **identifiers defined in RFC 6125, IPv4 address in CN or SAN** are matched to reference identifiers.

FCS_TLSC_EXT.2.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also **not implement any administrator override mechanism**.

FCS_TLSC_EXT.2.4 The TSF shall **present the Supported Elliptic Curves Extension with the following NIST curves: secp256r1, secp384r1, secp521r1 and no other curves** in the Client Hello.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

6.1.2.12 Extended: TLS Server Protocol with mutual authentication (FCS_TLSS_EXT.2)

FCS_TLSS_EXT.2.1 The TSF shall implement **TLS 1.2 ([RFC5246]☝), TLS 1.1 ([RFC4346]☝)** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- **TLS_RSA_WITH_AES_128_CBC_SHA as defined in [RFC3268]☝**
- **TLS_RSA_WITH_AES_256_CBC_SHA as defined in [RFC3268]☝**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in [RFC4492]☝**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in [RFC4492]☝**
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in [RFC4492]☝**
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in [RFC4492]☝**
- **TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5246]☝**
- **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in [RFC5246]☝**
- **TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5288]☝**
- **TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5288]☝**
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5289]☝**
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in [RFC5289]☝**
- **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]☝**
- **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]☝**
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]☝**
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]☝**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5289]☝**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in [RFC5289]☝**

.

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and **none**.

FCS_TLSS_EXT.2.3 The TSF shall **perform RSA key establishment with key size 2048 bits, 3072 bits ; generate EC Diffie-Hellman parameters over NIST curves secp256r1, secp384r1, secp521r1 and no other curves; generate Diffie-Hellman parameters of size 2048 bits, 3072 bits**.

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also **not implement any administrator override mechanism**.

FCS_TLSS_EXT.2.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

6.1.3 User data protection (FDP)

6.1.3.1 Subset information flow control (Traffic Filter) (FDP_IFC.1/TF)

FDP_IFC.1.1 / TF The TSF shall enforce the **Traffic Filter Flow Control Policy** on

- **Subjects: devices**
- **Information: IP packets**
- **Operation: transmit**

Application Note: *The definition of devices as a subject for this policy does not imply considering it as a subject for FAU_GEN.1.*

6.1.3.2 Simple security attributes (Traffic Filter) (FDP_IFF.1/TF)

FDP_IFF.1.1 / TF The TSF shall enforce the **Traffic Filter Flow Control Policy** based on the following types of subject and information security attributes:

- **Subject Security attributes:**
  - **Universal Network Profile (UNP) name**
- **Information security attributes:**
  - **source physical port;**
  - **destination physical port;**
  - **presumed network address of source subject;**
  - **presumed MAC address of source subject;**
  - **presumed network address of destination subject;**
  - **presumed MAC address of destination subject;**
  - **IP protocol**
  - **ICMP code**
  - **ICMP type**
  - **source VLAN id**
  - **source VLAN tag (802.1Q tagging)**
  - **source port number (for UDP or TCP);**
  - **destination port number (for UDP or TCP);**
  - **TCP flags and attributes (for TCP);**

FDP_IFF.1.2 / TF The TSF shall permit an information flow between a controlled subject and *another* controlled *subject* ~~information~~ via a controlled operation if the following rules hold:

- **if the physical source port has port-based Network Access Control enabled and a UNP name is bound as a result of authentication or device classification, all the information security attribute values are unambiguously permitted by the policy rules associated with the UNP;**

- **if the physical source port has port-based Network Access Control enabled but a UNP name cannot be bound as a result of authentication or device classification, all the information security attribute values are unambiguously permitted by the common policy rules (configured via QoS);**
- **if the physical source port has port-based Network Access Control disabled, all the information security attribute values are unambiguously permitted by the common policy rules (configured via QoS);**

Application Note: *A user or device can be associated with a UNP.*

Application Note: *Policy rules are composed by a condition are an action. Conditions may be composed from all possible combinations of the values of the subject and information security attributes, and membership to groups of physical ports (port groups), MAC addresses (MAC groups), network addresses (network groups), and combination of protocol and port (service groups). Actions can accept, drop or deny information flow.*

FDP_IFF.1.3 / TF The TSF shall enforce the **no additional information flow control rules.**

FDP_IFF.1.4 / TF The TSF shall explicitly authorize an information flow based on the following rules: **none**.

FDP_IFF.1.5 / TF The TSF shall explicitly deny an information flow based on the following rules:

- **if port-based Network Access Control is enabled on the physical source port and there is no UNP name or VLAN ID associated with the subject;**
- **if IP spoofing is enabled on the physical source port, and the presumed network address of the source subject, in the information, does not match the IP subnet for the port;**
- **if DHCP snooping and IP source filtering are enabled at the physical source port, and the presumed MAC and source network addresses of the IP packet do not match the MAC and network addresses of the subject obtained during the DHCP request (DHCP snooping binding table), or**
- **if the presumed network address of the destination subject does not match any entry in the routing table.**

6.1.3.3 Subset information flow control (VLAN) (FDP_IFC.1/VLAN)

FDP_IFC.1.1 / VLAN The TSF shall enforce the **VLAN Flow Control Policy** on

- **Subjects: devices;**
- **Information: IP packets;**
- **Operation: transmit**

Application Note: *The definition of devices as a subject for this policy does not imply considering it as a subject for FAU_GEN.1.*

6.1.3.4 Simple security attributes (VLAN) (FDP_IFF.1/VLAN)

FDP_IFF.1.1 / VLAN The TSF shall enforce the **VLAN Flow Control Policy** based on the following types of subject and information security attributes:

- **Subject Security attributes:**
  - **Universal Network Profile (UNP) name**
- **Information security attributes:**
  - **source physical port;**
  - **presumed network address of destination subject;**
  - **VLAN Tag (for 802.1Q traffic);**

.

FDP_IFF.1.2 / VLAN The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) **information flow is allowed to all physical ports associated with the VLAN corresponding to the VLAN ID (IP bridging);**

b) **if the VLAN corresponding to the VLAN ID has an IP interface, information flow is allowed through this IP interface (IP routing).**

FDP_IFF.1.3 / VLAN The TSF shall enforce the **no additional rules**.

FDP_IFF.1.4 / VLAN The TSF shall explicitly authorize an information flow based on the following rules: **none**.

FDP_IFF.1.5 / VLAN The TSF shall explicitly deny an information flow based on the following rules:

a) **if the packet includes a VLAN Tag (802.1Q), and the VLAN Tag does not match the default VLAN or any of the tagged VLANs associated with the physical port;**

b) **If the physical port is configured to support only tagged traffic and an untagged packet is received;**

c) **If the VLAN ID corresponds to a VLAN that is disabled.**

6.1.3.5 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to** the following objects **incoming packets**.

6.1.4 Identification and authentication (FIA)

6.1.4.1 Authentication Failure Management (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 1 and 999** unsuccessful authentication attempts occur related to **Administrators attempting to authenticate remotely using a password**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until the "user lockout unlock" command is taken**

by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed.

Application Note: *This functionality is not applicable for the "admin" user account.*

6.1.4.2 Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the *administrative* user while the authentication is in progress *at the local console*.

6.1.4.3 Password management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: **"@", "#", "$", "%", "^", "&", "*", "(", ")", “~”, “{“, “}”, “[“, ”]”, “:”, “;”, “|“, “\“, “/”, “.”, “<” and “>";**

b) Minimum password length shall be configurable to between **1** and **30** characters.

6.1.4.4 User Identification and authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

a) Display the warning banner in accordance with FTA_TAB.1;

b) **no other actions**.

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

6.1.4.5 Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1 The TSF shall provide a local **password-based** authentication mechanism to perform local administrative user authentication.

6.1.4.6 X.509 Certificate Validation (FIA_X509_EXT.1/Rev)

FIA_X509_EXT.1.1 / Rev The TSF shall validate certificates in accordance with the following rules:

- [RFC5280]☝ certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

- The TSF shall validate the revocation status of the certificate using **the Online Certificate Status Protocol (OCSP) as specified in [RFC6960], a Certificate Revocation List (CRL) as specified in [RFC5280] Section 6.3, Certificate Revocation List (CRL) as specified in [RFC5759] Section 5**
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

Application Note: *The TOE validates a certificate using the CRL stored in the flash filesystem. The TOE does not have the capability of downloading CRLs; they must be manually downloaded and updated by the administrator.*

FIA_X509_EXT.1.2 / Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.4.7 X.509 Certificate Authentication (FIA_X509_EXT.2)

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by [RFC5280] to support authentication for **TLS**, and **no additional uses**.

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall **not accept the certificate**.

Application Note: *Certificate revocation is verified by using an OCSP server and CRLs.*

6.1.4.8 Extended: X509 Certificate Requests (FIA_X509_EXT.3)

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by [RFC2986] and be able to provide the following information in the request: public key and **Common Name, Organization, Organizational Unit, Country**.

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.1.4.9 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following administrator configurable conditions:**

a) Minimum password length between 1 and 30 characters

b) Password age of 1-150 days

c) **Password cannot contain username**

d) **Password includes a minimum number of uppercase characters (the range is from 0-7 characters)**

e) **Password includes a minimum number of lowercase characters (the range is from 0-7 characters)**

f) **Password includes a minimum number of numeric characters (the range is from 0-7 characters)**

g) **Password includes a minimum number of non-alphanumeric characters (the range is from 0-7 characters)**

h) **Password must not be changed within a minimum number of days (the range is 0-150 days)**

6.1.4.10 End user and device attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users *and devices*: **username, password, MAC address, UNP**.

6.1.4.11 Timing of authentication of end users and devices (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow

- **information flow for unauthenticated end users and devices**

on behalf of the user *or device* to be performed before the user *or device* is authenticated.

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

Application Note: *Identification and Authentication are enforced on physical ports with port-based Network Access Control enabled and any of the authentication mechanisms enabled.*

6.1.4.12 Multiple authentication mechanisms for end users and devices (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide **the following authentication mechanisms:**

a) **MAC-based authentication (for devices);**

b) **IEEE 802.1x authentication (for users);**

c) **none**

to support user *and device* authentication.

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

- **if port-based Network Access Control is not enabled in the physical port, no authentication is performed;**
- **if port-based Network Access Control is enabled in the physical port, then:**
  - **if 802.1X authentication is enabled, then 802.1X authentication is performed;**
  - **if MAC-based authentication is enabled, then MAC-based authentication is performed;**

  - ○ **if 802.1X authentication is enabled to be performed after MAC-based authentication (either passing or failing), then 802.1X authentication is performed;**
  - ○ **if MAC-based authentication is enabled to be performed after 802.1X authentication fails, then MAC-based authentication is performed;**
  - ○ **if no authentication mechanism is enabled, then no authentication is performed.**

Application Note: *MAC-based authentication is for devices (non-supplicant devices), whereas 802.1X authentication is for users (supplicant devices). In either case, authentication is performed through a RADIUS server included in the operational environment.*

6.1.4.13 Timing of identification of end users and devices (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

- **information flow for unauthenticated end users and devices**

on behalf of the user *or device* to be performed before the user *or device* is identified.

FIA_UID.1.2 The TSF shall require each user *or device* to be successfully identified before allowing any other TSF-mediated actions on behalf of that user *or device*.

Application Note: *Identification and Authentication are enforced on physical ports with port-based Network Access Control enabled and any of the authentication mechanisms enabled.*

6.1.4.14 End user and device subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user *and device* security attributes with subjects acting on the behalf of that user *or device*: **VLAN ID, UNP name**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user *or device* security attributes with subjects acting on the behalf of users *or devices*:

- **if authentication succeeds, and there is a UNP name associated with the subject, then this UNP name is used;**
- **if authentication succeeds, and there is a VLAN ID associated with the subject, then this VLAN ID is used;**
- **if authentication succeeds but there is no UNP name or VLAN ID associated with the subject, then the UNP name or VLAN ID associated with the physical port authentication mechanism pass policy is used;**
- **if authentication is not possible (the external server is not reachable), and there is a UNP or VLAN associated with this scenario (server-down), then the UNP name or VLAN ID is used.**
- **if the subject cannot be bound to an UNP or VLAN (either authentication failed or the UNP is invalid):**
  - ○ **if classification rules are enabled on the physical port, and there is a rule that matches the attributes of the incoming packet, the UNP name or VLAN ID associated with the rule is used.**

- ○ **if classification rules are not enabled on the physical port or the previous classification fails (no matching rule is found), then the default UNP or VLAN associated with the physical port is used. If there is no default UNP or VLAN is defined, then no binding is performed.**

Application Note: *A classification rule can be based on the physical port, MAC address, network address and protocol of the incoming packet. It can be a rule that is part of a UNP.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user *and device* security attributes associated with subjects acting on the behalf of users *or devices*: **none**.

6.1.5 Security management (FMT)

6.1.5.1 Management of security functions behaviour (FMT_MOF.1/ManualUpdate)

FMT_MOF.1.1 / ManualUpdate The TSF shall restrict the ability to **enable** the functions **to perform manual updates** to **Security Administrators**.

6.1.5.2 Management of TSF data (FMT_MTD.1/CoreData)

FMT_MTD.1.1 / CoreData The TSF shall restrict the ability to **manage** the **TSF data** to **Security Administrators**.

6.1.5.3 Specification of management functions (FMT_SMF.1)

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

- **Ability to administer the TOE locally and remotely;**
- **Ability to configure the access banner;**
- **Ability to configure the session inactivity time before session termination or locking;**
- **Ability to update the TOE, and to verify the updates using hash comparison capability prior to installing those updates;**
- **Ability to configure the authentication failure parameters for FIA_AFL.1;**
- **Ability to configure audit behaviour;**
- **Ability to manage the cryptographic keys;**
- **Ability to configure the cryptographic functionality;**
- **Ability to re-enable an Administrator account;**
- **Ability to set the time which is used for time-stamps;**
- **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;**
- **Ability to import X.509v3 certificates to the TOE's trust store;**
- **Ability to configure VLANs and IP interfaces;**
- **Ability to configure the Traffic Filter and VLAN information flow control policies**

.

6.1.5.4 Restrictions on security roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Security Administrator**

.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

a) **The Security Administrator role shall be able to administer the TOE locally;**

b) **The Security Administrator role shall be able to administer the TOE remotely**

are satisfied.

6.1.5.5 Management of security functions behaviour (FMT_MOF.1/Services)

FMT_MOF.1.1 / Services The TSF shall restrict the ability to **enable, disable** *, start and stop* ~~the functions~~ **services** to **Security Administrators**.

6.1.5.6 Management of security functions behaviour (FMT_MOF.1/Functions)

FMT_MOF.1.1 / Functions The TSF shall restrict the ability to **determine the behaviour of , modify the behaviour of** the functions **transmission of audit data to an external IT entity, handling of audit data** to **Security Administrators**.

6.1.5.7 Management of TSF data (FMT_MTD.1/CryptoKeys)

FMT_MTD.1.1 / CryptoKeys The TSF shall restrict the ability to **manage** the **cryptographic keys** to **Security Administrators**.

6.1.5.8 Management of common security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the **Traffic Filter Flow Control Policy, VLAN Flow Control Policy** to restrict the ability to **change_default, query, modify, delete** the security attributes **declared in FDP_IFC.1/TF and FDP_IFC.1/VLAN** to **the security administrator**.

6.1.5.9 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Traffic Filter Flow Control Policy, VLAN Flow Control Policy**, to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **security administrator** to specify alternative initial values to override the default values when an object or information is created.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.6.2 Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.1.6.3 TSF testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests **during initial start-up (on power on)** to demonstrate the correct operation of the TSF: **power on self-tests required by the FIPS 140-2 standard in the OpenSSL cryptographic module**.

6.1.6.4 Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and **the most recently installed version of the TOE firmware/software**.

FPT_TUD_EXT.1.2 The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and **no other update mechanism**.

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a **published hash** prior to installing those updates.

6.1.6.5 Reliable Time Stamps (FPT_STM_EXT.1)

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

FPT_STM_EXT.1.2 The TSF shall **allow the Security Administrator to set the time**.

6.1.7 TOE access (FTA)

6.1.7.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate *a remote* interactive session after a **Security Administrator-configurable time interval of session inactivity**.

Application note: *This requirement is applicable to sessions regardless of whether the user has been already authenticated successfully or not (login prompt).*

6.1.7.2 User-initiated Termination (FTA_SSL.4)

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

6.1.7.3 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing ~~a~~ *an administrative* user session the TSF shall display ~~an~~ *a Security Administrator-specified* advisory *notice and consent* warning message regarding ~~unauthorised~~ use of the TOE.

6.1.7.4 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, **terminate the session** after a Security Administrator-specified time period of inactivity.

6.1.8 Trusted path/channels (FTP)

6.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall *be capable of using SSH, TLS to* provide a *trusted* communication channel between itself and ~~another trusted IT product~~ *authorized IT entities supporting the following capabilities: audit server, RADIUS authentication server, LDAP server, SSH client, SSH server, SFTP client, SFTP server, SNMPv3 protocol* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure *and detection of modification of the channel data*.

FTP_ITC.1.2 The TSF shall permit **the TSF, *or the authorized IT entities*~~another trusted IT product~~** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **sending audit records to the external syslog server, requesting user credentials to an LDAP server, requesting user authentication to a RADIUS authentication server, sending SSH and SFTP requests, sending and receiving IPv6 messages**.

Application Note: *The SSHv2 protocol is used for the SSH client, SSH server, SFTP client and SFTP server. TLSv1.1 and TLSv1.2 are used for protecting the communication with the RADIUS, LDAP and syslog external servers, and SNMPv3 peers.*

6.1.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall *be capable of using SSH to* provide a communication path between itself and *authorized* **remote** *Administrators* ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure** *and provides detection of modification of the channel data*.

FTP_TRP.1.2 The TSF shall permit **remote ~~users~~*Administrators*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial ~~user~~*Administrator* authentication , and all remote administration actions**.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT
FAU_GEN.2	O.AUDIT
FAU_STG.1	O.AUDIT
FAU_STG_EXT.1	O.AUDIT
FCS_CKM.1	O.CRYPTOGRAPHY
FCS_CKM.2	O.CRYPTOGRAPHY
FCS_CKM.4	O.CRYPTOGRAPHY
FCS_COP.1/DataEncryption	O.CRYPTOGRAPHY
FCS_COP.1/SigGen	O.CRYPTOGRAPHY
FCS_COP.1/Hash	O.CRYPTOGRAPHY
FCS_COP.1/KeyedHash	O.CRYPTOGRAPHY
FCS_RBG_EXT.1	O.CRYPTOGRAPHY
FCS_SSHC_EXT.1	O.COMMUNICATION_CHANNELS
FCS_SSHS_EXT.1	O.COMMUNICATION_CHANNELS
FCS_TLSC_EXT.2	O.COMMUNICATION_CHANNELS
FCS_TLSS_EXT.2	O.COMMUNICATION_CHANNELS
FDP_IFC.1/TF	O.MEDIATE
FDP_IFF.1/TF	O.MEDIATE
FDP_IFC.1/VLAN	O.MEDIATE
FDP_IFF.1/VLAN	O.MEDIATE
FDP_RIP.1	O.MEDIATE
FIA_AFL.1	O.ADMIN_ACCESS
FIA_UAU.7	O.ADMIN_ACCESS
FIA_PMG_EXT.1	O.STRONG_PASSWORDS
FIA_UIA_EXT.1	O.ADMIN_ACCESS

Security functional requirements	Objectives
FIA_UAU_EXT.2	O.ADMIN_ACCESS
FIA_X509_EXT.1/Rev	O.COMMUNICATION_CHANNELS
FIA_X509_EXT.2	O.COMMUNICATION_CHANNELS
FIA_X509_EXT.3	O.COMMUNICATION_CHANNELS
FIA_SOS.1	O.STRONG_PASSWORDS
FIA_ATD.1	O.MEDIATE
FIA_UAU.1	O.MEDIATE
FIA_UAU.5	O.MEDIATE
FIA_UID.1	O.MEDIATE
FIA_USB.1	O.MEDIATE
FMT_MOF.1/ManualUpdate	O.ADMIN_ACCESS, O.TRUSTED_UPDATES
FMT_MTD.1/CoreData	O.TSF_DATA_PROTECTION
FMT_SMF.1	O.ADMIN_ACCESS, O.AUDIT, O.STRONG_PASSWORDS, O.TRUSTED_UPDATES, O.TSF_DATA_PROTECTION
FMT_SMR.2	O.ADMIN_ACCESS, O.AUDIT, O.STRONG_PASSWORDS, O.TRUSTED_UPDATES, O.TSF_DATA_PROTECTION
FMT_MOF.1/Services	O.ADMIN_ACCESS
FMT_MOF.1/Functions	O.ADMIN_ACCESS, O.AUDIT, O.TSF_DATA_PROTECTION
FMT_MTD.1/CryptoKeys	O.ADMIN_ACCESS
FMT_MSA.1	O.MEDIATE
FMT_MSA.3	O.MEDIATE
FPT_SKP_EXT.1	O.TSF_DATA_PROTECTION
FPT_APW_EXT.1	O.TSF_DATA_PROTECTION
FPT_TST_EXT.1	O.SELF_TESTS
FPT_TUD_EXT.1	O.TRUSTED_UPDATES

Security functional requirements	Objectives
FPT_STM_EXT.1	O.AUDIT, O.COMMUNICATION_CHANNELS
FTA_SSL.3	O.ADMIN_SESSION
FTA_SSL.4	O.ADMIN_SESSION
FTA_TAB.1	O.ACCESS_BANNER
FTA_SSL_EXT.1	O.ADMIN_SESSION
FTP_ITC.1	O.COMMUNICATION_CHANNELS
FTP_TRP.1	O.COMMUNICATION_CHANNELS

Table 11: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objectives	Rationale
O.ADMIN_ACCESS	FIA_UIA_EXT.1 defines that the display of the banner is the only action allowed prior to identification and authentication. FIA_UAU_EXT.2 defines the password-based authentication mechanism, while FIA_UAU.7 requires that password feedback be obscured during authentication. The following SFRs restrict security management functionality to security administrators: FMT_MOF.1/ManualUpdate for Trusted Updates of the TOE, FMT_MOF.1/Functions for Audit functionality behaviour, FMT_MTD.1/CryptoKeys for management of cryptographic keys, and FMT_MTD.1/CoreData for management of TSF data. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.ADMIN_SESSION	FTA_SSL_EXT.1 and FTA_SSL.3 address the termination of local and remote sessions after a specified period of inactivity. FTA_SSL.4 address the termination of the session by the administrator.
O.CRYPTOGRAPHY	FCS_CKM.1 defines the required standards and key sizes for key generation, while FCS_CKM.2 defines the required standards for key distribution. FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash define the cryptographic algorithms, modes, key sizes and standards. FCS_RBG_EXT.1 defines the Deterministic Random Bit Generator (DRBG) and the minimum entropy required for key generation. FCS_CKM.4 defines the mechanisms for destroying cryptographic keys.

Security objectives	**Rationale**
O.COMMUNICATION_CHANNELS	FTP_ITC.1 and FTP_TRP.1 define trusted communication channels with external IT entities and remote administrators, respectively. Trusted communication channels are secured by the protocols mentioned below. Secure transport protocols are defined in FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.2 and FCS_TLSS_EXT.2. FIA_X509_EXT.1/Rev and FIA_X509_EXT.2 provides certificate validation for the TLS protocol. FIA_X509_EXT.3 defines the requirements for certificate request and response management. FPT_STM_EXT.1 provides reliable timestamps for validating certificates.
O.TRUSTED_UPDATES	FPT_TUD_EXT.1 specifies the behavior of the verification and installation of software updates by the TOE administrator. FMT_MOF.1/ManualUpdate, FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.AUDIT	FAU_GEN.1 defines the events that the TOE is required to audit. Those events are related to other security functional requirements showing which event contributes to make users accountable for their actions with respect to the requirement. FAU_GEN.2 requires that the events are associated with the identity of the user that caused the event. This association can only be established if the user is known, which is not the case for unsuccessful login attempts. FAU_STG_EXT.1 requires both the support of local storage for the audit trail and the transmission of the generated audit data to an external IT entity using a trusted channel. FAU_STG.1 protects the locally stored audit records from unauthorised deletion and modification. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective. FMT_MOF.1/Functions provides access control on audit management activities. FPT_STM_EXT.1 provides reliable timestamps for generating audit records.
O.TSF_DATA_PROTECTION	FPT_SKP_EXT.1 addresses the protection of cryptographic key material, whereas FPT_APW_EXT.1 addresses the protection of administrator passwords. FMT_MTD.1/CoreData, FMT_MTD.1/CryptoKeys, FMT_SMF.1 and FMT_SMR.2 specify security management functionality associated with this objective and its corresponding access constraints.
O.STRONG_PASSWORDS	FIA_PMG_EXT.1 and FIA_SOS.1 specify the administrative password policy that can be configured by TOE administrators. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.SELF_TESTS	FPT_TST_EXT.1 specifies the self-tests that the TOE executes at start-up (power-on self-tests) and during the execution of cryptographic services (conditional tests).

Security objectives	Rationale
O.ACCESS_BANNER	FTA_TAB.1 addresses the display of the banner before a session is established.
O.MEDIATE	FIA_UID.1, FIA_UAU.1 and FIA_UAU.5 address the identification and authentication mechanisms available for allowing dynamic binding of devices to VLANs and Universal Network Profiles (UNP). FIA_ATD.1 and FIA_USB.1 specifies the device attributes and binding rules. FDP_IFC.1/TF and FDP_IFF.1/TF address the enforcement of the Traffic Filter Flow Control Policy; FDP_IFC.1/VLAN and FDP_IFF.1/VLAN address the enforcement of the VLAN Flow Control Policy. FDP_RIP.1 also ensures that the internal buffers are cleared prior to allowing new information be stored into those buffers. FMT_MSA.1 and FMT_MSA.3 specifies the requirements for initializing and managing attributes for configuring the information flow control policies.

Table 12: Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of the SFRs modeled in CC Part 2 and [NDcPPv2.1]☝, and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UIA_EXT.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
	FTP_ITC.1	FTP_ITC.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1

Security functional requirement	Dependencies	Resolution
FCS_COP.1/DataEncryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1/SigGen	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1/Hash
	FCS_CKM.4	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1/Hash
FCS_COP.1/KeyedHash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_RBG_EXT.1	No dependencies	
FCS_SSHC_EXT.1	FCS_CKM.1	FCS_CKM.1
	FCS_CKM.2	FCS_CKM.2
	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash	FCS_COP.1/KeyedHash
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_SSHS_EXT.1	FCS_CKM.1	FCS_CKM.1
	FCS_CKM.2	FCS_CKM.2
	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash	FCS_COP.1/KeyedHash
	FCS_RBG_EXT.1	FCS_RBG_EXT.1

Security functional requirement	**Dependencies**	**Resolution**
FCS_TLSC_EXT.2	FCS_CKM.1	FCS_CKM.1
	FCS_CKM.2	FCS_CKM.2
	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash	FCS_COP.1/KeyedHash
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_TLSS_EXT.2	FCS_CKM.1	FCS_CKM.1
	FCS_CKM.2	FCS_CKM.2
	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash	FCS_COP.1/KeyedHash
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FDP_IFC.1/TF	FDP_IFF.1	FDP_IFF.1/TF
FDP_IFF.1/TF	FDP_IFC.1	FDP_IFC.1/TF
	FMT_MSA.3	FMT_MSA.3
FDP_IFC.1/VLAN	FDP_IFF.1	FDP_IFF.1/VLAN
FDP_IFF.1/VLAN	FDP_IFC.1	FDP_IFC.1/VLAN
	FMT_MSA.3	FMT_MSA.3
FDP_RIP.1	No dependencies	
FIA_AFL.1	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_PMG_EXT.1	No dependencies	
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1
FIA_UAU_EXT.2	No dependencies	
FIA_X509_EXT.1/Rev	FIA_X509_EXT.2	FIA_X509_EXT.2
FIA_X509_EXT.2	FIA_X509_EXT.1	FIA_X509_EXT.1/Rev

Security functional requirement	Dependencies	Resolution
FIA_X509_EXT.3	FCS_CKM.1	FCS_CKM.1
	FIA_X509_EXT.1	FIA_X509_EXT.1/Rev
FIA_SOS.1	No dependencies	
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1/ManualUpdate	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/CoreData	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FMT_MOF.1/Services	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MOF.1/Functions	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/CryptoKeys	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/TF FDP_IFC.1/VLAN
	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.2
FPT_SKP_EXT.1	No dependencies	
FPT_APW_EXT.1	No dependencies	
FPT_TST_EXT.1	No dependencies	

Security functional requirement	Dependencies	Resolution
FPT_TUD_EXT.1	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
FPT_STM_EXT.1	No dependencies	
FTA_SSL.3	No dependencies	
FTA_SSL.4	No dependencies	
FTA_TAB.1	No dependencies	
FTA_SSL_EXT.1	FIA_UAU.1	FIA_UIA_EXT.1
FTP_ITC.1	No dependencies	
FTP_TRP.1	No dependencies	

Table 13: TOE SFR dependency analysis

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are defined in [CC] part 3 for the Evaluation Assurance Level 2, augmented by ALC_FLR.2.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3	No	No	No	No
	ADV_TDS.1 Basic design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.2 Use of a CM system	CC Part 3	No	No	No	No
	ALC_CMS.2 Parts of the TOE CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ALC_FLR.2 Flaw reporting procedures	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.1 Evidence of coverage	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3	No	No	No	No

Table 14: SARs

6.4 Security Assurance Requirements Rationale

The chosen assurance level, EAL2, ensures the TOE to be resistant to an attacker possessing a Basic attack potential, commensurate with the threat environment that is experienced by typical consumers of the TOE. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. Additionally, the product vendor has specific customer requests for the evaluation of the TOE at this assurance level. These potential customers of the product vendor have determined for their own networks that an EAL2 evaluation of the product will provide satisfactory assurance.

EAL2 is augmented with ALC_FLR.2 to assist in ensuring that discovered security flaws are tracked and are corrected by the developer and that TOE users are aware of how to report a security flaw and receive corrective fixes.

7 TOE Summary Specification

7.1 TOE Security Functionality

This section presents a description of how the TOE SFRs are satisfied, organized by security function.

- Auditing
- Cryptographic Support
- Identification and Authentication of TOE Administrators
- Identification and Authentication of end users and devices
- Traffic Mediation
- Security Management
- Protection of the TSF
- Trusted Path/Channels

7.1.1 Auditing

Audit functionality in the TOE is provided via the switch logging feature, which records audit events for all administrative operations performed. Each audit record contains the date and time of the event, type of event, subject identity (whenever possible) and outcome (success or failure). The type of event and outcome are included in the Log Message field which specifies the condition recorded.

For certificate management (generation, import, update, deletion, view and verification of certificates; update of CRL), the audit record includes the full "aaa certificate" command line entered by the administrator, which provides the certificates and/or keys involved in the operation, and whether the operation succeeded or failed. The audit record also includes the description of the error in case of a failure.

The TOE supports the severity levels detailed in Table 15.

Security Level	Type	Description
1 *(highest severity)*	Alarm	A serious, non-recoverable error has occurred and the system must be rebooted.
2	Error	System functionality is reduced.
3	Alert	A violation has occurred.
4	Warning	A unexpected, non-critical event has occurred.
5	Event	A clear readable customer event.
6 *(default)*	Info	Any other non-debug message.
7	Debug1	A normal event debug message.
8	Debug2	A debug-specific message.
9 *(lowest severity)*	Debug3	A maximum verbosity debug message.

Table 15: TOE audit record levels

Security level 6 (Info) is enabled for all events by default and is the minimum severity level required in the evaluated configuration.

When an audit event request is made, the severity level on the request is compared to the severity level assigned to the application ID for which the event occurs. If the severity level of the log request is less than or equal to that of the application ID, the log message is generated and placed in the log file.

Specific security and administrative events that are required to be audited by this ST are generated with security level 6 (Info) and their description prefixed with the "EVENT-AUDIT". It is possible to configure the severity level either globally for all applications or on a per application basis.

The TOE can be configured to send records to an audit file on the flash file system, display them on the serial console, and/or send them to a remote syslog server.

For local permanent storage, audit data is stored in the audit file set located in the flash file system and prefixed as "swlog_". Whenever the audit file reaches a configurable threshold (maximum size for audit files), the audit file overwrites the data present in the oldest audit file of a set of circular audit files (in case the set of audit files is full). The amount of audit data that can be generated depends on the maximum size allowed for each of the audit files, which can be changed using the command: **`swlog output flash file-size <size in KB>`**. The TOE also provides a mechanism to display a warning to the user if the storage capacity has reached 90% of the configured size in any of the audit files.

Audit files are protected from modification and deletion by enforcing access control on groups of commands. Only the Security Administrator has privileges to clear the audit records.

The following table shows the number of circular files that comprise the audit file set, the file names for the audit file set, the parameter used to define the maximum size allowed for audit records, and the default value and allowed range for that parameter.

Operating System	Number of circular files	Audit file set	Parameter definition	Default value	Allowed values
AOS 8.6.4.R11	Eight	swlog_<suffix>[3], swlog_<suffix>.0 through swlog_<suffix>.6	Maximum size for each file (in KB)	1250KB	125KB to 12500KB

Table 16: Audit permanent storage

The TOE can also transfer audit data to an external audit server, implemented with a syslog server. A secure communication channel is established between the TOE and the external audit server using TLSv1.1 or TLSv1.2 in order to protect audit data communication from loss of integrity or confidentiality.

An audit record is sent to the audit server immediately after the event occurs. If communication fails, the audit event is only recorded locally and is not resent; the TOE tries to reconnect to the audit server whenever a new audit generation request is received.

7.1.1.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

[3] this suffix depends on the Omniswitch model.

FAU_GEN.1

The audit functionality generates records for the auditable events specified in this SFR, including the general information required as well as the specific information required for each event.

FAU_GEN.2

Whenever possible, the audit functionality includes the user id that caused the event (some of the audit events do not have a user associated, e.g. failure in establishing a TLS session).

FAU_STG_EXT.1

Audit events are stored locally in the flash memory using a circular chain of audit files. Whenever the audit file reaches a configurable threshold (maximum size for audit files), the audit file overwrites the data present in the oldest audit file of a set of circular audit files (in case the set of audit files is full).

The audit functionality can be also configured to send the audit events to an external syslog server using TLS for protecting the communication channel.

FAU_STG.1

The audit files are protected from deletion and modification. Only the Security Administrator can clear the audit records.

7.1.2 Cryptographic Support

The TOE implements cryptographic protocols and algorithms using the following standard packages included in the TOE.

- OpenSSL v1.0.2s and OpenSSL FIPS Object Module SE v2.0.16 for TLSv1.1, TLSv1.2, and cryptographic algorithm support
- OpenSSH v7.7p1 for implementing the SSHv2 protocol. OpenSSH uses OpenSSL for the underlying cryptographic algorithms

7.1.2.1 OpenSSL cryptographic module

The TOE includes OpenSSL, which implements versions 1.1 and 1.2 of the Transport Layer Security (TLS) protocol and provides general-purpose cryptographic services. The following table summarizes the cryptographic algorithms implemented in OpenSSL and used by the TOE to support communication protocols, protection of TSF data and authentication.

Cryptographic Services	Cryptographic Algorithms and Key Sizes	Usage / Purpose
Key Generation	RSA 2048-bit and 3072-bit keys	• TLSv1.1 and TLSv1.2 • SSHv2
	ECDSA P-256, P-384 and P-521 keys	• SSHv2
	ECDSA P-256, P-384 and P-521 ephemeral keys	• TLSv1.1 and TLSv1.2 • SSHv2
	Diffie-Hellman keys	• SSHv2
Key Establishment	RSA-based, 2048-bit and 3072-bit keys	• TLSv1.1 and TLSv1.2 • SSHv2

Cryptographic Services	Cryptographic Algorithms and Key Sizes	Usage / Purpose
	ECDSA-based, P-256, P-384 and P-521 keys	• TLSv1.1 and TLSv1.2 • SSHv2
Encryption / Decryption	AES in CBC mode, 128 and 256 bit keys	• TLSv1.1 and TLSv1.2 • SSHv2
	AES in CTR mode, 128 and 256 bit keys	• SSHv2
	AES in GCM mode, 128 and 256 bit keys	• TLSv1.1 and TLSv1.2 • SSHv2
Signature Generation and Verification	RSA PKCS#1 v1.5 with SHA-1, SHA-256, SHA-384 and SHA-512, using 2048-bit and 3072-bit keys	• TLSv1.1 and TLSv1.2 • SSHv2
	ECDSA with SHA-256, SHA-384 and SHA-512 using NIST P-256, P-384, and P-521 curves.	• TLSv1.1 and TLSv1.2 • SSHv2
Message Digest	SHA-1	• Signature Generation and Verification • Keyed Hashing
	SHA-256	• Signature Generation and Verification • Keyed Hashing • Password storage • Trusted Update
	SHA-384	• Keyed Hashing
	SHA-512	• Keyed Hashing
Keyed Hashing	HMAC-SHA-1 with 160-bit key	• TLSv1.1 and TLSv1.2 • SSHv2 • MAC-based device authentication
	HMAC-SHA-256 with 256-bit key	• TLSv1.1 and TLSv1.2 • SSHv2
	HMAC-SHA-384 with 384-bit key	• TLSv1.1 and TLSv1.2
	HMAC-SHA-512 with 512-bit key	• SSHv2
DRBG	Hash_DRBG (default), CTR_DRBG, HMAC_DRBG	• Asymmetric key generation • Session key generation

Table 17: Cryptographic Services and Algorithms

The following table provides additional information on the HMAC parameters supported by OpenSSL and used in the TOE:

Cryptographic Algorithm	Hash function	Block size (hash function)	Key Size	Output MAC length
HMAC-SHA-1	SHA-1	512 bits	256 bits	96 and 160 bits
HMAC-SHA-256	SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-384	SHA-384	1024 bits	256 bits	384 bits
HMAC-SHA-512	SHA-512	1024 bits	256 bits	512 bits

Table 18: HMAC parameters

OpenSSL includes a Deterministic Random Bit Generator (DRBG) used for key generation and random data (e.g. shared secrets). The DRBG uses the HASH_DRBG with SHA-256 algorithm by default; if there is a failure in the instantiation, the DRBG will fallback to CTR_DRBG, and then to HMAC_DRBG.

The module uses a Non-Deterministic Random Number Generator (NDRNG) as the entropy source for seeding the DRBG. The NDRNG is provided by the operating system kernel and based on HAVEGE (Hardware Volatile Entropy Gathering and Expansion) that uses the uncertainties which appear in the behavior of the processor when interrupts occur. The NDRNG provides at least 256 bits of entropy.

OpenSSL performs the following power-up self-tests to ensure that the module and all validated cryptographic algorithms work properly:

- Integrity verification of the shared libraries that comprise the cryptographic module;
- Known Answer Test (KAT) for symmetric encryption and decryption algorithms;
- KAT for the DRBG;
- KAT for MAC and message digest algorithms;
- KAT for RSA signature generation and verification algorithms;
- KAT for the Elliptic Curve Diffie-Hellman algorithm;
- Pair-wise Consistency Tests (PCT) for ECDSA asymmetric algorithms (consisting of performing signature generation and verification for a known ECDSA key..

OpenSSL also performs the following conditional tests during the execution of services:

- PCT on each generation of an RSA key pair, consisting of performing signature generation and verification of a predefined message using the generated RSA key pair, as well as public key encryption and private key decryption of a predefined message using the generated RSA key pair.
- PCT on each generation of an ECDSA key pair, consisting of performing signature generation and verification of a predefined message using the generated ECDSA key pair.

In case of failure of any of the power-up self-tests or conditional tests, OpenSSL raises an exception and the TOE shows an error message in the console, for instance:

"*Signature RSA test Failed Incorrectly!!*"

or

"*DRBG SHA256 test Failed Incorrectly!!*"

Once all self-tests are executed, and in case a failure was identified, OpenSSL shows a summary of the errors encountered and forces the TOE to restart. The following is the list of possible error messages:

"*FIPS routines:FIPS_check_incore_fingerprint:fingerprint does not match:fips.c:232:*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=SHA1 Digest*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=SHA1 Digest*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=SHA1 Digest*"

"*FIPS routines:FIPS_selftest_aes:selftest failed:fips_aes_selftest.c:98:*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=RSA SHA256 PSS*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=ECDSA P-224*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=DSA SHA384*"

OpenSSL maintains all secret keys, private keys, public keys, certificates and other critical security parameters (CSP) used by the cryptographic services (DRBG internal state, session keys, etc.) requested by the TOE in random access memory (RAM) during the life-time of the cryptographic operation. All CSPs are in RAM in plaintext form; OpenSSL clears with zeroes and deallocates all the memory used by the CSP when they are no longer needed (e.g. the cryptographic handler is freed or a TLS session is finished).

7.1.2.2 Transport Layer Security (TLS) protocol

The TOE implements versions 1.1 and 1.2 of the TLS protocol provided by OpenSSL. The TOE establishes a secure channel using TLS for the following purposes:

- As a TLS client
  - Communication with an external audit server (syslog) for audit storage.
  - Communication with an external LDAP server for using authentication credentials stored externally.
  - Communication with a RADIUS server for external authentication.
  - Communication with an SNMP Management Station for sending SNMP notifications.
- As a TLS server
  - Communication with an SNMP Management Station for receiving SNMP requests.

The TOE allows mutual authentication, both for client and server sides, through the use of X.509 certificates. The TOE performs certificate and certificate path validation of the server certificate during the TLS handshake. If the certificate cannot be successfully validated (e.g. it has expired or has been revoked) the TLS session is not established. See section 7.1.2.4 for more information.

When acting as a client, for single authentication, it is the server end who presents the certificate during TLS handshake, so when acting as a client, the TOE only parses the certificate from the TLS message and verifies that the server certificate is valid. For mutual authentication, though, the TOE also has to send the client certificate at the server's request. The TOE looks for the certificate and its private key at the certificate directory (/flash/switch/cert.d). Table 19 lists the naming conventions for certificates used in SNMP communication and the rest of the communication with external entities.

When acting as a client, the TOE verifies that the certificate presented by the TLS server during the TLS handshake corresponds to the server, using one of the following methods:

- Verify that the DNS names included in the Subject Alternative Name (SAN) field as the reference identifier for the server certificate matches the server hostname, according to [RFC6125]☝.
- Verify that the IPv4 address included in either the Subject Alternative Name (SAN) or Common Name (CN) fields matches server IPv4 address.

If any of the verification methods succeeds, then the certificate is trusted. Otherwise, the TLS session is not established.

Similarly, when acting as a server, the TOE verifies that the certificate presented by the TLS client during the TLS handshake corresponds to the client, using the following method:

- Verify that the content included in the Distinguished Name (DN) or Subject Alternative Name (SAN) field matches the expected identifier for the client.
- Verify that the IPv4 address included in either the Subject Alternative Name (SAN) or Common Name (CN) fields matches server IPv4 address (IPv6 is not supported). The TOE converts the IPv4 address by parsing the CN and storing the binary representation in an internal data structure (canonical format is not enforced).

If the verification method succeeds, then the certificate is trusted. Otherwise, the TLS session is not established.

The TOE only allows the establishment of a TLS secure channel using TLSv1.1 or TLSv1.2. The TOE denies any attempt by a TLS client to establish communication using the following versions of the SSL or TLS protocols: SSLv2.0, SSLv3.0 or TLSv1.0.

The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL. The TOE destroys session keys when the session is terminated by clearing with zeroes and deallocating the RAM memory used to store the session keys.

The TOE supports the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The cipher suites are selected in the order shown in the list. In addition, the administrator can restrict the cipher suites that the TOE shall use via management functions (e.g. **`ssl cipher`** CLI command).

The TOE implements the Supported Elliptic Curves Extension according to [RFC4492]☝ with NIST curves secp256r1, secp384r1, and secp521r1. This behaviour is performed by default and there is no security management function to disable it.

Key agreement parameters used for server key exchange by ECDHE cipher suites are determined based on the selected NIST curve, as described in [RFC8422]☝.

For destruction of plaintext keys in volatile storage, the TOE relies on the functionality provided by OpenSSL to zeroize and release the memory allocated for cryptographic operations. For keys in non-volatile storage, the TOE provides CLI commands to remove the relationship between keys and certificates and their usage in the TOE.

The following table shows the cryptographic keys involved in the TLS protocol, their location and how they are created and destroyed:

Certificate / Key	Certificate / Key Location	Purpose	Destruction

TOE client certificate (public and private keys)	`/flash/switch/cert.d/myCliCert.pem (or .crt)`
	`/flash/switch/cert.d/myCliPrivate.key`
		TOE authentication (TOE acting as client)	Removal from filesytem through CLI commands

TOE client/server certificate (public and private keys) of SNMP local identity	`/flash/switch/cert.d/<aluSubagent>.pem (or .crt)`
	`/flash/switch/cert.d/<aluSubagent>.key`
		TOE authentication (TOE acting as client or server for SNMP)	Removal from filesytem through CLI commands

TOE client/server certificate (public key) of SNMP remote identity	`/flash/switch/cert.d/<cert-name>.pem (or .crt) (e.g. manager.crt)`	External entity authentication (TOE acting as client or server for SNMP) Key establishment	Removal from filesytem through CLI commands
External Entity server certificate (public key)	RAM (received from TLS server)	External Entity authentication (TOE acting as client) Key establishment	Zeroization and deallocation when session is terminated
External Entity client certificate (public key)	RAM (received from TLS client)	External entity authentication (TOE acting as server)	Zeroization and deallocation when session is terminated

Certificate / Key	Certificate / Key Location	Purpose	Destruction
Session keys (shared secrets, ephemeral keys, encryption keys, data authentication keys)	RAM	Integrity and confidentiality during session	Zeroization and deallocation when session is terminated

Table 19: Certificates and keys used by the TLS protocol

7.1.2.3 Secure Shell version 2 (SSHv2) protocol

The TOE implements the Secure Shell version 2 (SSHv2) protocol using OpenSSH v7.7p1. The package uses OpenSSL as the underlying layer for cryptographic algorithms.

The TOE establishes a secure channel using SSHv2 for the following purposes.

- As a SSHv2 server
  - Secure communication for SSHv2 clients used in Security Management (Command Line Interface)
  - Support for Secure File Transfer protocol (SFTP) clients
- As a SSHv2 client
  - Secure communication with remote SSH servers
  - SFTP client for remote SFTP servers

The SSHv2 protocol complies with [RFC4251], [RFC4252], [RFC4253], [RFC4254], [RFC4344], [RFC5656], [RFC6668] and [RFC8332]. The TOE also implements Diffie-Hellman group 14 and group 16 in accordance with [RFC3526] section 3.

The following table shows the algorithms used for the different aspects of the SSHv2 protocol in the AOS supported by the TOE.

SSHv2 protocol aspect	Cryptographic Algorithm
Authentication Methods	Public-key based using RSA PKCS#1 v1.5 and ECDSA (see public key algorithms)
	Password based using SHA-256.
Key Establishment (key exchange)	Diffie Hellman group 14 with SHA-1, group 14 with SHA-256 and group 16 with SHA-512
	Elliptic Curve Diffie Hellman with SHA-256, SHA-384 and SHA-512, and NIST curves P-256, P-384 and P-521
Encryption algorithms	AES (CBC mode) with 128-bit and 256-bit keys
	AES (CTR mode) with 128-bit and 256-bit keys
	AES (GCM mode) with 128-bit and 256-bit keys
Public key algorithms	RSA PKCS#1 v1.5 with SHA-1, SHA-256 and SHA-512, using 2048-bit and 3072-bit keys.

SSHv2 protocol aspect	Cryptographic Algorithm
	ECDSA with SHA-256, SHA-384 and SHA-512, and NIST curves P-256, P-384 and P-521
Data integrity MAC algorithms	HMAC-SHA1, HMAC-SHA1-96
	HMAC-SHA-256
	HMAC-SHA-512

Table 20: SSHv2 algorithms supported by the TOE

The TOE does not implement any optional characteristics, with the exception of the cryptographic algorithms mentioned in Table 20 that are marked as "OPTIONAL" in the aforementioned RFCs.

The TOE (acting as a SSHv2 server) supports SSHv2 sessions using SSH public key and password authentication by default. When a user attempts to establish a SSHv2 session, the TOE verifies that the user has a public key associated and the public key file exists (`/flash/switch/.profiles/.<username>_keys.pub`). If these conditions are met, then public key authentication is used, otherwise password authentication is used as the fallback authentication mechanism.

In addition, the TOE provides the **`ssh enforce pubkey-auth`** command in the CLI to enforce public key authentication only, thus disabling password based authentication. If public key authentication fails, then access to the TOE is not granted.

When starting a SSHv2 session as a client in the TOE, the authentication mechanisms to be used in the session are enforced by the SSHv2 server. The TOE supports both SSH public key and password authentication. For SSH public key authentication, the `ssh`command issued by the administrator from the CLI must include the user's private key as a parameter and the key must exist in the flash filesystem.

The TOE limits the size of SSHv2 packets to 256 Kb; packets greater than this size in an SSH transport connection are dropped. In addition, the TOE also controls that the SSHv2 session does not transmit more than 2^{28} packets with the same session key. If that threshold is surpassed, new session keys are established between both ends.

The TOE creates session keys following the SSHv2 protocol specification and using the DRBG implemented in OpenSSL. The TOE destroys session keys when the session is terminated by clearing with zeroes and deallocating the Random Access Memory (RAM) memory used to store the session keys.

SSHv2 public and private keys are created by the TOE administrator via the CLI. Keys are also deleted from the filesystem by the TOE administrator using filesystem commands from the CLI (e.g. rm). The TOE removes from the filesystem the file entry corresponding to the key .

For destruction of plaintext keys in volatile storage, the TOE relies on the functionality provided by OpenSSL to zeroize and release the memory allocated for cryptographic operations. For keys in non-volatile storage, the TOE provides CLI commands to remove the relationship between keys and certificates and their usage in the TOE.

The following table shows the cryptographic keys involved in the SSHv2 protocol, their location and how they are created and destroyed:

Key	Key Location	Purpose	Destruction
SSH host RSA public key	/flash/system/ssh_host_rsa_key.pub	Key Establishment	Removal from filesytem through CLI commands
SSH host RSA private key	/flash/system/ssh_host_rsa_key	Key Establishment	
SSH host ECDSA public key	/flash/system/ssh_host_ecdsa_key.pub	Key Establishment	
SSH host ECDSA private key	/flash/system/ssh_host_ecdsa_key	Key Establishment	
SSH user public key	/flash/system/<username>_rsa.pub	Public Key authentication	
SSH user private key	/flash/system/<username>_rsa	Public Key authentication	
Session keys (shared secrets, encryption keys, data authentication keys)	RAM	Integrity and confidentiality during session	Zeroization and deallocation when session terminates

Table 21: Keys used by the SSHv2 protocol

7.1.2.4 X.509 Certificate generation and validation

The TOE supports X.509 certificate validation and certificate path validation according to [RFC5280]☝. They are used during the TLS handshake procedure to verify trust on the certificate received from the external IT entity, and verify the trust of the OCSP responder (if applicable).

When acting as a TLS client, the TOE parses and validates the TLS server certificate. If mutual authentication is required, the TOE sends the certificate used for that purpose (see table 19) that is located at the certificate directory (/flash/switch/cert.d).

When acting as a TLS server, the TOE presents the certificate used for that purpose (see table 19) that is located at the certificate directory (/flash/switch/cert.d). The TOE forces mutual authentication thus it requests, parses and validates the TLS client certificate.

Certificate validation and certificate path validation consist of the following steps:

1. Verify that the certificate has a correct format and has not expired.
2. Verify that the chain of trust from the certificate up to the CA root certificate is maintained.
3. Verify that the basicConstraints extension exists and the CA flag is set to TRUE for all CA certificates in the path.
4. Verify that the CA root certificate is trusted.
5. Verify that the certificate has not been revoked.
6. Verify that the extendedKeyUsage field in the certificate corresponds to the use of the certificate ("Client Authentication", "Server Authentication", "OCSP Signing" purpose).

If all these steps are successful, then the certificate is considered valid. If any of these steps fails, then the certificate is considered invalid.

Certificate pinning is not supported by the TOE.

The TOE obtains the revocation status of the certificate by validating first the certificate using the local CRL file (crl.pem) stored in the flash filesystem ("/flash/switch/cert.d"). If the local CRL is not configured, then the OCSP responder is attempted. If the OCSP responser is not reachable (*Unknown* status) or if the OCSP URL is not present in the certificate, then the validation fails and the certificate is assumed to be revoked. In either case, if the mechanism chosen for obtaining the certificate revocation status is available (i.e. the OCSP responds *OK* or *Revoked*, or the local CRL is properly configured), then the result is used to determine whether the certificate is revoked or not. As described above, whenever the mechanism is not available (the OCSP service does not responds or the CRL file does not exist), the TOE assumes the certificate status is revoked.

The TOE contains a default CA keystore located in the flash filesystem ("/flash/switch/ca.d"). This keystore is used to perform certificate validation and contains all CA root certificates that are trusted by the TOE. The same directory contains the CRL used for local validation of the certificate revocation.

The TOE supports generation of RSA-based certificates. The TOE includes commands in the CLI to generate a Certificate Signing Request (CSR) and receive the corresponding CA certificate response file. After the CSR file is generated by the TOE, the administrator sends the request to a CA for being signed. Once the CA certificate response is received, the administrator uses the CLI to validate the certificate chain and import the signed certificate into the TOE.

RSA-based as well as ECDSA-based certificates can be generated outside the TOE and imported and configured in the TOE using the CLI.

The TOE provides the **`certificate delete`** command in the CLI to remove certificates and their associated keys from the filesystem.

7.1.2.5 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FCS_CKM.1
The TOE generates RSA and ECDSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1 and TLSv1.2; and RSA, ECDSA and Diffie-Hellman assymetric cryptographic keys that are used to protect communications for SSHv2.

FCS_CKM.2
The TOE performs key establishment based on RSA and ECDSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1 and TLSv1.2; and RSA, ECDSA and Diffie-Hellman assymetric cryptographic keys that are used to protect communications for SSHv2.

FCS_CKM.4
The TOE destroys key material by overwriting it with zeroes and releasing the allocated memory only after a read-verify to ensure it was properly zeroized.

FCS_COP.1/DataEncryption
OpenSSL and the kernel crypto library implement AES encryption and decryption in accordance to these SFRs.

FCS_COP.1/SigGen
OpenSSL implements RSA and ECDSA signature generation and verification in accordance to these SFRs.

FCS_COP.1/Hash

OpenSSL implements SHA-1 and the SHA-2 family hashing algorithms in accordance to these SFRs.

FCS_COP.1/KeyedHash

OpenSSL and the kernel crypto library implement HMAC keyed hashing algorithm with SHA-1 and the SHA-2 family in accordance to these SFRs.

FCS_RBG_EXT.1

OpenSSL implements DRBG algorithms in accordance to this SFR. The TOE provides an entropy source for seeding the DRBG with a minimum of 256 bits.

FCS_SSHC_EXT.1

OpenSSH implements the SSHv2 protocol in accordance to these SFRs.

FCS_SSHS_EXT.1

OpenSSH implements the SSHv2 protocol in accordance to these SFRs.

FCS_TLSC_EXT.2

OpenSSL implements the TLSv1.1 and TLSv1.2 protocols in accordance to these SFRs. The TOE supports the cipher suites selected in these SFRs.

FCS_TLSS_EXT.2

OpenSSL implements TLSv1.1 and TLSv1.2 protocols in accordance to these SFRs. The TOE supports the cipher suites selected in these SFRs.

FIA_X509_EXT.1/Rev

The TOE performs X.509 certificate validation using the Online Certificate Status Protocol (OCSP), as specified in [RFC6960]☝, and using a Certificate Revocation List (CRL), as specified in [RFC5759]☝.

FIA_X509_EXT.2

The TOE supports X.509 certificate validation for the TLSv1.1 and TLSv1.2 protocols.

FIA_X509_EXT.3

The TOE supports the generation of Certificate Request Messages as specified by [RFC2986]☝ and processing of the CA Certificate Response.

7.1.3 Identification and Authentication of TOE Administrators

The TOE provides local and remote access to administrators; local access is provided through the serial console (connected to the available ports), whereas remote access is provided through the SSHv2 protocol using an SSH or SFTP client. Both local and remote sessions can be terminated by the administrator at any time.

Before a local or remote session is established, a banner is displayed to the user that attempts to log into the TOE. An administrator of the TOE can modify the content of this banner to display warnings or advisory notices that reflect the security policy of the organization.

The TOE requires the administrator to identify and authenticate to the TOE prior to accessing any of the management or secure transfer functionality, regardless of the mechanism being used to interface with the TOE (e.g. serial console, SSH, SFTP).

There is one default user account provided with the TOE: *admin*. The *admin* user account is the initial administrator assigned all privileges. The *admin* user account is used to install and setup the TOE.

The TOE can perform identification and authentication locally (using either its local database or an LDAP database server residing in the operational environment) or via an external authentication server in the operational environment. Once identification and authentication succeeds with the credentials provided by the user, the TOE grants access to the user by showing the command line interface (CLI) prompt.

7.1.3.1 Local Authentication

When configured for local authentication, the TOE maintains administrative-user security attributes of identifier (user ID), password information (authentication data), and user privileges (authorizations or user profile) and roles. The authentication data (password) is hashed prior to being stored using SHA-256. These attributes are stored locally on the flash file system, in directories protected from read and write access from the administration console.

If the user and password information entered by the user match the authentication data (either stored locally in the TOE or in the LDAP database server), authentication succeeds and the TOE grants access to the user.

The TOE provides the following user authentication failure settings:

- *Lockout window*: The length of time a failed user login attempt is aged before it is no longer counted as a failed user login attempt. The valid range is 0 to 99,999. The number of failed login attempts is decremented by the number of failed attempts that age beyond the lockout window. The default lockout window is set to 0, which means that all consecutive failed login attempts are counted, regardless of how much time has elapsed between the failed logins.
- *Lockout threshold*: The number of failed user login attempts allowed within a given lockout window period of time (1-999). The default lockout threshold is set to 0, which means that there is no limit to the number of failed login attempts allowed, but this value is not allowed in the evaluated configuration.
- *Lockout duration*: The length of time a user account remains locked out until it is automatically unlocked. The valid range is 0 to 99,999. The default lockout duration is set to 0, which means that there is no automatic unlocking of a user account by the TOE.

The TOE ensures that if the number of failed user login attempts exceeds the lockout threshold during the lockout window period of time, the user account is locked out of the TOE for the lockout duration. The user is unlocked when:

- the lockout duration expires, or
- an administrator unlocks the user via the `user lockout unlock` CLI command.

In either case, the user’s authentication failure counter is reset when the user successfully authenticates.

The TOE monitors the time of inactivity of local and remote sessions, forcing the termination of a session when the timeout interval has been reached.

- The login attempt session timeout defines the amount of time the administrator can take to accomplish a successful login to the TOE. If the login timeout period is exceeded, the TCP connection is closed by the TOE. The default login timeout period is 55 seconds.
- The user session timeouts define the amount of time the user can be inactive for CLI and SFTP sessions. When the TOE detects no user activity for the administrator configured period of time, the user is logged off the TOE. The default timeout for CLI and SFTP sessions is four minutes.

The TOE provides global password settings used to implement and enforce local password complexity when a password is created or modified. The password settings available on the TOE are:

- *Minimum Password Length*: The number of characters required when configuring a user password. The default value is 15 characters and can be changed within the range of 1 to 30 characters.
- *Password Expiration*: The number of days before user passwords will expire. The allowed range is 1-150 days. Password expiration is disabled by default.
- *Username not allowed*: Specifies whether or not the password is allowed to contain the username. The default is to allow the password to contain the username.
- *Minimum Uppercase characters*: Specifies the minimum number of uppercase characters required for a user password. The allowed range is 0-7. By default, there is no required minimum number of uppercase characters.
- *Minimum Lowercase characters*: Specifies the minimum number of lowercase characters required for a user password. The allowed range is 0-7. By default, there is no required minimum number of lowercase characters.
- *Minimum Numeric characters*: Specifies the minimum number of numeric characters (base-10 digits) required for a user password. The allowed range is 0-7. By default, there is no required minimum number of numeric characters.
- *Minimum non-alpha characters*: Specifies the minimum number of non-alphanumeric characters (symbols) required for a user password. The allowed range is 0-7. By default, there is no required minimum number of non-alpha characters.
- *Password History*: Specifies the maximum number of old passwords to retain. The range is 0-24 and the default is to retain 4 old passwords. The user is prevented from reusing any retained passwords. A value of 0 disables the password history function.
- *Minimum Password Age*: Specifies the minimum number of days during which the user is prevented from changing a password. The allowed range is 0-150. By default, there is no required minimum number of days.

When authentication is performed through a local session, the TOE does not display the password characters; instead, an asterisk is echoed for each character input.

7.1.3.2 External authentication

The TOE supports the use of a RADIUS server for external authentication. The external authentication server is responsible for storing and maintaining the user’s security attributes, as well as the policies for password quality and locking of users after unsuccessful login attempts.

The TOE sends the user and password information provided by the user that is attempting to login; the external authentication server then verifies the credentials and returns the result of the identification and authentication operation. If authentication succeeds, the TOE grants access to the user.

7.1.3.3 SNMP authentication

The TOE also allows remote access to an SNMP Management Station; in this case, the TOE implements the SNMPv3 protocol with the Transport Security Model (TSM) over the TLS protocol to provide authentication, integrity and confidentiality via TLS mutual authentication.

If the client certificate provided by the SNMP Management Station attempting to connect to the TOE is successfully verified by the TOE as part of the TLS mutual authentication, identification and authentication succeeds and the TOE accepts the communication session between the SNMP Management Station (acting as a SNMP Manager) and the TOE (acting as the SNMP agent).

7.1.3.4 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FIA_AFL.1
The TOE prevents the establishment of a remote session after a defined number of unsuccessful attempts using the password-based authentication method.

FIA_PMG_EXT.1, **FIA_SOS.1**
The TOE allows the configuration of a password policy that includes a minimum length, and the combination of upper and lower case, numbers and special characters.

FIA_UIA_EXT.1
The TOE displays a warning banner before an administrative user attempts to login through a local (serial) or remote (SSHv2 client) console.

FIA_UAU_EXT.2, **FIA_UAU.7**
The TOE provides a password-based authentication mechanism, where passwords are not shown during the identification and authentication process.

FTA_SSL_EXT.1
The TOE terminates local sessions after a period of inactivity.

FTA_SSL.3
The TOE terminates remote sessions after a period of inactivity.

FTA_SSL.4
An Administrator can terminate a local or remote session at any time.

FTA_TAB.1
The TOE displays a banner containing advisory notice and consent warning message before an interactive session is established.

7.1.4 Identification and Authentication of end users and devices

The TOE provides port-based network access control on devices using the following authentication mechanisms: IEEE 802.1x authentication (for supplicant devices) and MAC-based authentication (for non-supplicant devices). The ultimate purpose of identification and authentication of devices is to associate the connection with a VLAN ID and a UNP, through which the TOE can enforce the VLAN and traffic filtering information flow control policies, which can be different from unauthenticated connections.

IEEE 802.1X authentication verifies the identity of a user in the end user device or supplicant. Upon detection of the supplicant, access to the TOE is enabled and set to an "unauthorized" state. In this state, only 802.1X traffic from the device is allowed; other network traffic is blocked. Next, the TOE (authenticator) sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the TOE (authenticator) forwards to the RADIUS authentication server (which is part of the operational environment). The TOE verifies whether authentication succeeded, failed, or the external authentication could not be performed. If authentication succeeded, the TOE sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant ends its session, it sends an EAP-logoff message to the TOE. The TOE then sets the port to the "unauthorized" state thereby blocking all non-EAP traffic.

Note: *IEEE 802.1X is the recommended solution to provide the highest level of security for end user device authentication.*

MAC-based authentication verifies the identity of the device. The TOE receives the incoming packet and creates a request for a RADIUS server using the source MAC address included in the packet as both the username and the password of the request. The TOE sends the request to the RADIUS server and verifies whether authentication succeeded, failed, or external authentication could not be performed.

Both authentication mechanisms can coexist; which authentication mechanisms are enabled, in which order they are applied and what actions are taken when the authentication succeeds, fails or is unavailable depends on the rules defined by the administrator. For instance, regardless of what is connected to a port in the TOE (hubs, IP phones, etc.), every device can be identified and authenticated. When managed devices that are capable of 802.1X authentication attempt to connect to the network they will be challenged to provide their credentials. Other legacy devices such as printers will not be challenged, but instead will be granted access through MAC authentication.

Both authentication mechanisms require the use of a RADIUS server as an external authentication server, which is part of the operational environment.

A UNP can be associated with the device in the corresponding entry in the RADIUS database. This security attribute determines the enforcement of the VLAN and Traffic Filtering information control policies on all traffic coming from the authenticated device. Additional rules are provided in the TOE for situations in which this attribute cannot be obtained or is invalid.

- A default value when MAC-based authentication succeeds but does not return a VLAN ID or UNP value.
- A default value when 802.1X authentication succeeds but does not return a VLAN ID or UNP value.
- A default value when authentication cannot be performed (e.g. external authentication server is down or unreachable).
- Device classification rules when authentication fails or the port is not configured to enforce authentication (but port-based network access control is enforced). Classification rules can be based on the MAC address, network address, protocol of the incoming packet. If a matching rule is found, the associated VLAN ID or UNP value is chosen.
- A default value when device classification is not configured for the port, or no matching classification rule is found.

7.1.4.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FIA_UID.1, FIA_UAU.1, FIA_UAU.5
The TOE determines whether the end user and/or device must be authenticated or not based on the configuration of the physical source port (whether port access control is enabled or not, and whether MAC-based or 802.1X authentication are enabled.

FIA_ATD.1, FIA_USB.1
For physical ports that has network access control enabled, the TOE binds a UNP name and VLAN ID to the device based on the result of the authentication (success, failure, unavailable), and classification rules.

7.1.5 Traffic Mediation

The TOE provides two coexisting mechanisms of traffic mediation: VLANs and Traffic Filtering.

7.1.5.1 VLAN Flow Control

The TOE controls bridging and routing of frames received using a security policy based on the concept of VLAN.

VLANs provides a mechanism to segment network traffic within a network switch restricting IP bridging within the same VLAN. Creating a VLAN bridging domain across multiple switches and/or stacks of switches also allows VLAN members to communicate with each other even if they are not connected to the same physical switch. Additionally, adding or removing devices from a VLAN can be performed through port assignment configuration, without the need of physically changing a network device connection or location.

A VLAN is identified by a unique number, known as the VLAN ID. VLAN 1 is the default VLAN in the TOE. All ports have VLAN 1 as the default VLAN for the port.

The TOE also supports the IEEE 802.1Q standard for tagged packets. Tagged packets include a Logical Network identification (VLAN Tag), indicating which VLAN they are a member of. Ports of the TOE, in addition of the default VLAN, can have one or more tagged VLANs assigned. This method allows the TOE to bridge traffic for multiple VLANs over one physical port connection.

When a packet is received on a port, the TOE first determines the VLAN to be assigned:

- For fixed ports, an untagged packet is assigned to the default VLAN assigned to the port. A tagged packet is assigned to the VLAN informed in the VLAN tag.
- For non-fixed ports, the VLAN is determined based on the following:
    - End user or device authentication mechanisms (IEEE 802.1X, MAC-based, respectively) and authentication result (success, failure, not available). As a result, the non-fixed port is eventually associated with a VLAN (through an association with an UNP.
    - VLAN Tag included in the packet (if any).
    - Classification rules based on packet attributes (MAC address, IP address, protocol). As a result, the non-fixed port is eventually associated with a VLAN (through an association with an UNP).

Once the VLAN is assigned to the incoming packet, the VLAN ID is inserted in the packet and the traffic filtering policy (described in next section) is applied. If the result of applying the traffic filtering policy is to allow traffic, the packet is then bridged to other ports that are assigned to the same VLAN ID. Once the assignment occurs, a VLAN port association (VPA) is created. The TOE keeps track of the VPAs existing between each port and VLAN, in order to know to which physical ports the packet has to be bridged.

The following rules also apply:

- If a fixed port is configured to support only tagged traffic and an untagged packet is received, then the packet is dropped.
- If a fixed port receives a tagged packet with a VLAN ID that is not the default VLAN for the port and is not any of the tagged VLANs assigned to the port (if any), then the packet is dropped.
- if the VLAN is disabled, then the packet is dropped.

If a device needs to communicate with another device that belongs to a different VLAN, the TOE mediates the flow of information between the VLANs using IP forwarding (i.e., routing). This forwarding function is based on internal routing tables. These routing tables are 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. The following routing protocols are permitted:

- IPv4 Routing Protocols: OSPF, RIPv2, BGP, VRRP, VRRP2
- IPv6 Routing Protocols: OSPFv3, RIPng, VRRP3

If a VLAN does not have an IP interface, the ports associated with that VLAN are in essence firewalled from other VLANs.

7.1.5.2 Traffic Filtering

Once an incoming packet is assigned to a VLAN, the TOE can enforce a traffic filtering policy based on the security attributes of subject and the contents of the IP packet. The TOE checks if there are any policies that match the conditions of the flow. If there are no policies that match the flow, the flow is permitted or denied based on the global disposition value. By default, the TOE is configured to permit (route) all packets that do not match a policy. The global disposition value can be changed by the administrator.

The TOE controls Layer-2 and Layer-3/4 traffic that is allowed to flow through the TOE, imposing a security policy to filter the traffic. Traffic is filtered using Access Control Lists (ACLs) stored in the policy database. The TOE examines each network packet received to determine whether to route or drop the packet based on the rules specified by the administrator in the ACLs. The rules in the ACL can be based on the following attributes:

- source and destination physical ports defined by chassis, slot and port numbers (which can also be declared in port groups)
- presumed source and destination MAC addresses (which can also be defined in MAC groups)
- presumed source and destination IP addresses (which can also be defined in network groups)
- IP protocol
- ICMP code and type
- source VLAN ID
- source and destination port number (for UDP or TCP)
- TCP flags and attributes (for TCP)

In addition to the rules that comprise the default policy list, similar traffic filtering rules can be defined for end-user devices in UNPs. A UNP can be dynamically associated to non-fixed ports after end-user device authentication, and ACL rules defined in the UNP are enforced in all incoming traffic from that port.

The policies are assigned precedence which defines the order in which the rules are checked and what actions are taken if there is a conflict. If a flow matches more than one policy, the policy with the highest precedence is applied to the flow. If a flow matches more than one policy with the same precedence values, the rule configured first takes precedence. Rules can also be configured to enable logging of use of the rule and to define the severity level assigned to the event.

The TOE also rejects packets arriving on a network interface if the presumed address of the source belongs to a different network interface, providing the ability to reject packets with forged IP source addresses (IP spoofing).

The TOE also implements DHCP snooping, a technique through which the TOE maintains a table (DHCP snooping table) containing the MAC address and the physical port from where a DHCP request frame was received and the IP address assigned by the DHCP server (which is part of the operational environment). If IP source filtering is enabled, the TOE verifies that incoming IP packets coming from the same device maintains the same information; otherwise, the packets are dropped.

7.1.5.3 Residual Information

The TOE ensures that residual information is unavailable to other resources by overwriting areas of memory that store any incoming packet data.

When packets arrive on the TOE's network interface they are written into memory. The TOE overwrites information previously stored in that memory location with the newly received packet. Pointers are used by AOS to identify the beginning and ending of each packet in memory. The correct use and operation of these pointers ensures that data from a prior packet stored in memory is not inadvertently included in a later packet or available for use.

7.1.5.4 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FDP_IFC.1/TF, **FDP_IFF.1/TF**
The TOE enforces information flow control based on Traffic Filtering rules.

FDP_IFC.1/VLAN, **FDP_IFF.1/VLAN**
The TOE enforces information flow control based on VLAN information.

FDP_RIP.1
The TOE ensures that residual information is unavailable to other resources by overwriting areas of memory that store any incoming packet data.

7.1.6 Security Management

The TOE provides the following management functions for use by security administrators.

- Set the date and time
- Configure the access banner for local and remote login sessions
- Configure session inactivity time for login sessions
- Install TOE firmware updates with the capability of verifying the integrity of those updates
- Configure authenticate failure parameters for login sessions (e.g. unsuccessful authentication attempts)
- Configure audit behaviour
- Configure user login attempt lockout settings
- Re-enable an Administrator account
- Configure password policy settings
- Manage cryptographic keys
- Configure cryptographic functionality
- Manage the trust store and X509.v3 certificates (designate certificates as trust anchors, import X.509v3 certificates)
- Configure VLANs and IP interfaces

- Create, delete and modify all items corresponding to the Traffic Filter Flow Control Policy and the VLAN Flow Control Policy

The security management functions can be performed through a CLI. The CLI can be accessed from the serial console or through a SSHv2 client. In addition, the Flash file system on the TOE provides the ability to store and edit configuration files that can be transferred to and from the Flash file system via SFTP.

Acting on behalf of a security administrator, the CLI requests security management operations from the same underlying service in the TOE. Therefore, although there are different methods of use for requesting the security management functions, each method utilizes the same underlying software to actually perform the functions.

Use of each of these management functions is restricted to the authorized administrator by requiring the administrator to successfully identify and authenticate to the TOE prior to allowing access to the functions. Administrators are granted access to management functions based on the access granted to their user account. The TOE provides the ability to grant read-only or read-write access to the command families available in the CLI. Examples of command families include file, system, config, module, interface, ip, vlan, dns, qos, policy, session, aaa. The aaa command family provides the ability to configure the type of authentication methods supported by the TOE and perform user account management.

The associated global disposition value determines the default values for security attributes used by the information flow control policies. By default, the TOE is configured to permit (route) all packets that do not match a policy. The global disposition values can be changed by the administrator. The administrator is instructed in administrator guidance to set default attribute values in a secure manner as necessary for the deployed environment.

The TOE also supports the SNMPv3 protocol for TOE management. An SNMP Management Station (acting as an SNMP Manager) connects to the TOE (acting as an SNMP agent) and requests or changes configuration parameters using Get, GetNext, GetBulk or Set operations. Parameters are modeled as MIB objects in the Management Information Bases (MIBs) provided by the TOE and included in each command of the CLI reference guide [AOS8-CLI].

The TOE (acting as an SNMP agent) can also send unsolicited messages (traps or informs) to the SNMP Management Station to notify the manager of network conditions.

The TOE implements SNMP with the Transport Security Model (TSM) using the TLS protocol in accordance with [RFC3411]☝, [RFC5591]☝ and [RFC5953]☝. The TSM model provides identification, authentication and protection of the SNMP communication between peers through the establishment of a TLS session using mutual authentication.

All management functionality can be performed entirely either through the CLI or MIB objects through SNMP.

7.1.6.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FMT_MOF.1/Functions
The TOE restricts security administrators to determine and modify the behavior of audit functionality.

FMT_MOF.1/ManualUpdate
The TOE restricts security administrators to perform manual updates of the TOE software.

FMT_MTD.1/CoreData
The TOE restricts security administrators to manage TSF data.

FMT_MTD.1/CryptoKeys
The TOE restricts security administrators to manage cryptographic keys.

FMT_SMF.1
The TOE provides the security management functions specified in this SFR.

FMT_SMR.2
The TOE supports the Security Administrator role, who is the only role authorized to access the TOE locally and remotely.

FMT_MSA.1, **FMT_MSA.3**
The TOE provides permissive default values for the security attributes that comprise the Traffic Filter and VLAN security functional policies. In addition, the TOE restricts security administrators to specify alternative initial values or modify values for these attributes.

7.1.7 Protection of the TSF

Passwords are stored in non-plaintext form using a hashing algorithm: SHA-256. The hashed value of the password is stored in a directory of the flash filesystem protected from read and write access.

The TOE includes the OpenSSL cryptographic module, which supports the TLS protocol and the underlying cryptographic algorithms used by the TOE. The module performs power-on self-tests (POST) to ensure the integrity of the module itself and the correct behavior of the cryptographic algorithms, and conditional tests to ensure that asymmetric key pairs are correctly generated. The POST proceeds until all self-tests are completed. In case of a failure in any of the self-tests, the TOE writes an error message to the console, and is forced to reload and reinitialize the operating system, thus performing the POST again. This mechanism ensures that no cryptographic algorithm is available until all self-tests are successful. Please refer to section 7.1.2.1 for a detailed description of the self-tests and the error messages that the module shows when the self-tests fail.

The TOE prevents access to all pre-shared keys, symmetric keys and private keys from the CLI by using operating system's file access control: access to directories containing files with sensitive material is denied for all configured administrative users. The admin user, which is the default user in the TOE, is the only user that can have access to the files but its use is restricted to the installation and the initial configuration of the TOE.

The TOE does not provide a mechanism for automatic updates of the TOE. The administrator is responsible of following the instructions included in the TOE guidance to securely download, and install and/or update the TOE.

The TOE provides via the CLI several commands for installing and updating the TOE in a secure way:

- Download the new version of the TOE and the corresponding SHA-256 hash value (firmware image and hash value files) from the vendor's secure website.
- Visualize the currently active version of the TOE, and the most recently installed version of the TOE (`show microcode` command).
- Verify the integrity of the downloaded image file that represents the TOE firmware against the SHA-256 hash value contained in a hash file[4] (`image integrity-check` command).

[4] the hash file must be created by the administrator

- Reload the TOE using the new version of the TOE firmware, verifying its integrity against the SHA-256 hash value contained in a hash file (`reload from` command).

When the TOE firmware is reloaded (`reload from` command), if the integrity of the TOE image is verified successfully, the command can proceed and the new version of the TOE is installed. If the integrity verification fails, then the TOE image is rejected and the command does not proceed with the update.

The TOE does not provide a means for installing a trusted update of the TOE with a delayed activation. However, the administrator must reboot the TOE in order to make the changes effective.

The TOE provides a reliable date and time for the following security functions:

- Generation of a timestamp for audit events.
- Verification of the expiration of the certificate in X.509 certificate validation.
- Calculation of period of inactivity of an interactive session to evaluate the termination of local and remote sessions.

The TOE obtains the date and time from an internal system clock. This system clock can be updated by the security administrator through the CLI.

7.1.7.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FPT_SKP_EXT.1
The TOE stores key material in directories of the flash filesystem which are protected from read/access from any user, including administrators.

FPT_APW_EXT.1
The TOE stores the hashed value of the password in a directory of the flash filesystem that is protected from read/access from any user, including administrators.

FPT_TST_EXT.1
OpenSSL performs self-tests during start-up and conditional tests, which ensures the correct operation of the cryptographic algorithms.

FPT_TUD_EXT.1
The TOE allows administrators to verify the executing version and the most recently installed version of the TOE software. It also allows manual updates of the TOE software, verifying its trust and integrity using a published hash before being installed.

FPT_STM_EXT.1
The TOE has an internal system clock which is used to generate reliable timestamps for security related purposes like auditing and certificate validation.

7.1.8 Trusted Path/Channels

The TOE uses the service of external IT entities to support different aspects of the security functionality. The TOE ensures that communications between the TOE itself and these external IT entities are protected using a trusted communication channel.

The TOE also provides a trusted communication path using the SSHv2 protocol for sessions remotely initiated by administrators.

The following table summarizes the services used by the TOE and how they are protected.

Purpose	External IT entity	Secure channel
External storage of audit records	Syslog server	TLSv1.1 or TLSv1.2
External authentication	RADIUS server	TLSv1.1 or TLSv1.2
External storage for credentials	LDAP server	TLSv1.1 or TLSv1.2
Management of the TOE	SNMP Management Station	TLSv1.1 or TLSv1.2
SSH requests	SSH client/server	SSHv2
SFTP requests	SFTP client/server	SSHv2

Table 22: Trusted channels

7.1.8.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FTP_ITC.1

All communications between the TOE and external IT entities are protected using a secure channel via TLSv1.1, TLSv1.2 or SSHv2 protocols.

FTP_TRP.1

All communications initiated by remote administrators to the TOE are protected using a secure channel via the SSHv2 protocol.

8 Abbreviations, Terminology and References

8.1 Abbreviations

CAVP
Cryptographic Algorithm Validation Program

AC
Alternating Current

ACL
Access control List

AES
Advanced Encryption System

AH
Authentication Header

AIA
Authority Information Access

ALE
Alcatel-Lucent Enterprise

AOS
Alcatel-Lucent Operating System

ARM
Advanced RISC Machine

ASA
Authenticated Switch Access

ASIC
Application-Specific Integrated Circuit

BGP
Border Gateway Protocol

BOOTP
Bootstrap Protocol

CBC
Cipher Block Chaining

CFM
Chassis Fabric Module.

CLI
Command Line Interface

CMM
Chassis Management Module. Physically a separate blade for 9000 series switches. Logically a separate piece of functionality built into the Management of the 6850E series

CN
Common Name

CRL
Certificate Revocation List

CSP
Critical Security Parameter

CSR
Certificate Signing Request

DC
Direct Current

DCB
Data Center Bridging

DHCP
Dynamic Host Configuration Protocol

DNS
Domain Name Server

DRBG
Deterministic Random Bit Generator

DSA
Digital Signature Algorithm

DVMRP
Distance Vector Multicast Routing Protocol

EAP
Extensible Authentication Protocol

ECD
Extended Component Definition

ECDH
Elliptic Curve Diffie-Hellman

ECDHE
Elliptic Curve Diffie-Hellman Exchange

ECDSA
Elliptic Curve Digital Signature Algorithm

EMC
Electromagnetic Compatibility

EMI
Electromagnetic Interference

ESD
Electrostatic Discharge

ESP
Encapsulating Security Payload

GigE
Gigabit Ethernet

GNI
Gigabit Ethernet Network Interface

HDMI
High-Definition Multimedia Interface

HMAC
Keyed-Hash Message Authentication Code

HPoE
High Power over Ethernet

HTTPS
Hypertext Transfer Protocol Secure

IEEE
Institute of Electrical and Electronics Engineers

IGMP
Internet Group Management Protocol

IKE
Internet Key Exchange

IP
Internet Protocol

IPv4
Internet Protocol version 4

IPv6
Internet Protocol version 6

KAT
Known Answer Test

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

NI
Network Interface

NTP
Network Time Protocol

OCSP
Online Certificate Status Protocol

OS6465
Alcatel-Lucent Enterprise OmniSwitch 6465 Series with AOS 8.6.4.R11

OS6560
Alcatel-Lucent Enterprise OmniSwitch 6560 Series with AOS 8.6.4.R11

OS6860
Alcatel-Lucent Enterprise OmniSwitch 6860 Series with AOS 8.6.4.R11

OS6865
Alcatel-Lucent Enterprise OmniSwitch 6865 Series with AOS 8.6.4.R11

OS6900
Alcatel-Lucent Enterprise OmniSwitch 6900 Series with AOS 8.6.4.R11

OS9900
Alcatel-Lucent Enterprise OmniSwitch 9900 Series with AOS 8.6.4.R11

OSPF
Open Shortest Path First

PAE
Port Access Entity

PCB
Printer Circuit Board

PCT
Pair-wise Consistency Test

PIM
Protocol-Independent Multicast

PoE
Power over Ethernet

PoH
Power over HD Base-T

PTP
Precision Time Protocol

QNI
40-Gigabit Ethernet Network Interface

QoS
Quality of Service

QSFP
Quad Small Form-factor Pluggable

RADIUS
Remote Authentication Dial In User Service

RIP
Routing Information Protocol

RSA
Rivest Shamir Adleman (cryptosystem)

SAN
Subject Alternative Name

SFP
Small Form-factor Pluggable transceiver (used in section 1.5.2.1.1) or Security Function Policies (used in the rest of the ST)

SFTP
Secure File Transfer Protocol

SLB
Server Load Balancing

SNMP
Simple Network Management Protocol

SPB
Shortest Path Bridging

SPBM
Shortest Path Bridging MAC

SPD
Security Policy Database

SPI
Security Parameter Index

SSH
Secure Shell

SSHv2
Secure Shell version 2

STP
Spanning Tree Algorithm and Protocol

TACACS+
Terminal Access Controller Access-Control System Plus

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TSM
Transport Security Model

UDP
User Datagram Protocol

UNP
Universal Network Profile

USB
Universal Serial BUS

VC
Virtual Chassis

VFL
Virtual Fabric Link

VIP
Virtual IP

VLAN
Virtual LAN

VoIP
Voice Over IP

VXLAN
Virtual Extensible Local Area Network

XNI
10-Gigabit Ethernet Network Interface

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrative-user
An administrative user of the TOE, authorized to control TOE settings, as opposed to end-users, associated with general network traffic.

Appletalk
AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP)

Application
In the context of AOS auditing there are several ‘applications’ that log records. These are identified by a number and abbreviation.

CAVP
The NIST Cryptographic Algorithm Validation Program provides validation testing of Approved (i.e., FIPS-approved and NIST-recommended) cryptographic algorithms and their individual components.

Decnet
DECNET Phase IV (6003) protocol.

End-user
Network traffic, non-administrative users of the TOE.

Fixed-configuration Switch
A network switch where the number of ports cannot be changed, when compared to a chassis type product.

IEEE 802.1X
IEEE 802.1X is an IEEE Standard for port-based Network Access Control.

MAC Address
Media Access Control Address, also known as the hardware or adaptor address.

Port Mobility
The ability for the Alcatel-Lucent Switches to dynamically tag incoming traffic into a specific VLAN irrespective of the physical port the traffic enters.

Power over Ethernet
Power over Ethernet (PoE) provides inline power directly from the switch’s Ethernet ports. Powered Devices (PDs) such as IP phones and wireless APs can be powered directly from the switch’s RJ-45 ports.

Stackable Switch

Network switch that can be connected with a special function cable with other stackable switches to function as a virtual chassis using a central management point.

UNP

A Universal Network Profile comprises a set of policies that can be dynamically assigned to physical devices or end-users via authentication or by matching predefined criteria.

VLAN, (Virtual LAN) / Logical Network

The term VLAN was specified by IEEE 802.1Q; it defines a method of differentiating traffic on a LAN by tagging the Ethernet frames. By extension, VLAN is used to mean the traffic separated by Ethernet frame tagging or similar mechanisms. In this ST Logical network and VLAN are used interchangeably.

WebView

The web based GUI to manage the TOE.

8.3 References

AOS8-ARC **OmniSwitch AOS Release 8 Advanced Routing Configuration Guide**
Version Part No. 060607-10 Rev. A
Date July 2019

AOS8-CCGUIDE **Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS Release 8.6.R11**
Version Part No. 060612-00 Rev. A
Date December 2020

AOS8-CLI **OmniSwitch AOS Release 8 CLI Reference Guide**
Version Part No. 060609-10 Rev. A
Date July 2019

AOS8-DCS **OmniSwitch AOS Release 8 Data Center Switching Guide**
Version Part No. 060608-10 Rev. A
Date July 2019

AOS8-NC **OmniSwitch AOS Release 8 Network Configuration Guide**
Version Part No. 060606-10 Rev. A
Date July 2019

AOS8-RN **Release Notes - Rev. A - OmniSwitch 6465, 6560, 6860(E)/6865/6900/9900**
Version Part No. 033413-00 Rev. A
Date July 2019

AOS8-SM **OmniSwitch AOS Release 8 Switch Management Guide**
Version Part No. 060610-10 Rev. A
Date July 2019

AOS8-TCV **OmniSwitch AOS Release 8 Transceivers Guide**
Version Part No. 060611-10 Rev. A
Date July 2019

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R5
Date April 2017
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

NDcPPv2.1 **collaborative Protection Profile for Network Devices Version 2.1**
Version 2.1
Date 2019-03-11
Location https://www.niap-ccevs.org/MMO/PP/CPP_ND_V2.1.pdf

OS6465-HWUG **OmniSwitch 6465 Hardware Users Guide**
Version Part No. 060510-10, Rev. E
Date July 2019

OS6560-HWUG **OmniSwitch 6560 Hardware Users Guide**
Version Part No. 060474-10, Rev. F
Date July 2019

OS6860-HWUG **OmniSwitch 6860/6860E Hardware Users Guide**
Version Part No. 060390-10, Rev. H
Date July 2019

OS6865-HWUG **OmniSwitch 6865 Hardware Users Guide**
Version Part No. 060435-10, Rev L
Date July 2019

OS6900-HWUG **OmniSwitch 6900 Hardware Users Guide**
Version Part No. 060334-10, Rev. P
Date March 2019

OS9900-HWUG **OmniSwitch 9900 Series Hardware Users Guide**
Version Part No. 060409-10, Rev H
Date July 2019

RFC2986 **PKCS #10: Certification Request Syntax Specification Version 1.7**
Author(s) M. Nystrom, B. Kaliski
Date 2000-11-01
Location http://www.ietf.org/rfc/rfc2986.txt

RFC3268 **Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)**
Author(s) P. Chown
Date 2002-06-01
Location http://www.ietf.org/rfc/rfc3268.txt

RFC3411 **An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks**
Author(s) D. Harrington, R. Presuhn, B. Wijnen
Date 2002-12-01
Location http://www.ietf.org/rfc/rfc3411.txt

RFC3526 **More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)**
Author(s) T. Kivinen, M. Kojo
Date 2003-05-01
Location http://www.ietf.org/rfc/rfc3526.txt

RFC4251 **The Secure Shell (SSH) Protocol Architecture**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4251.txt

RFC4252 **The Secure Shell (SSH) Authentication Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4252.txt

RFC4253 **The Secure Shell (SSH) Transport Layer Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4253.txt

RFC4254 **The Secure Shell (SSH) Connection Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4254.txt

RFC4344 **The Secure Shell (SSH) Transport Layer Encryption Modes**
Author(s) M. Bellare, T. Kohno, C. Namprempre
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4344.txt

RFC4346 **The Transport Layer Security (TLS) Protocol Version 1.1**
Author(s) T. Dierks, E. Rescorla
Date 2006-04-01
Location http://www.ietf.org/rfc/rfc4346.txt

RFC4492 **Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)**
Author(s) S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller
Date 2006-05-01
Location http://www.ietf.org/rfc/rfc4492.txt

RFC5246 **The Transport Layer Security (TLS) Protocol Version 1.2**
Author(s) T. Dierks, E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5246.txt

RFC5280 **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
Author(s) D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk
Date 2008-05-01
Location http://www.ietf.org/rfc/rfc5280.txt

RFC5288 **AES Galois Counter Mode (GCM) Cipher Suites for TLS**
Author(s) J. Salowey, A. Choudhury, D. McGrew
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5288.txt

RFC5289 **TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)**
Author(s) E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5289.txt

RFC5591 **Transport Security Model for the Simple Network Management Protocol (SNMP)**
Author(s) D. Harrington, W. Hardaker
Date 2009-06-01
Location http://www.ietf.org/rfc/rfc5591.txt

RFC5656 **Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer**
Author(s) D. Stebila, J. Green
Date 2009-12-01
Location http://www.ietf.org/rfc/rfc5656.txt

RFC5759 **Suite B Certificate and Certificate Revocation List (CRL) Profile**
Author(s) J. Solinas, L. Zieglar
Date 2010-01-01
Location http://www.ietf.org/rfc/rfc5759.txt

RFC5953 **Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)**
Author(s) W. Hardaker
Date 2010-08-01
Location http://www.ietf.org/rfc/rfc5953.txt

RFC6125 **Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)**
Author(s) P. Saint-Andre, J. Hodges
Date 2011-03-01
Location http://www.ietf.org/rfc/rfc6125.txt

RFC6668 **SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol**
Author(s) D. Bider, M. Baushke
Date 2012-07-01
Location http://www.ietf.org/rfc/rfc6668.txt

RFC6960 **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**
Author(s) S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams
Date 2013-06-01
Location http://www.ietf.org/rfc/rfc6960.txt

RFC8017 **PKCS #1: RSA Cryptography Specifications Version 2.2**
Author(s) K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch
Date 2016-11-01
Location http://www.ietf.org/rfc/rfc8017.txt

RFC8332 **Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol**
Author(s) D. Bider
Date 2018-03-01
Location http://www.ietf.org/rfc/rfc8332.txt

RFC8422 **Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier**
Author(s) Y. Nir, S. Josefsson, M. Pegourie-Gonnard
Date 2018-08-01
Location http://www.ietf.org/rfc/rfc8422.txt