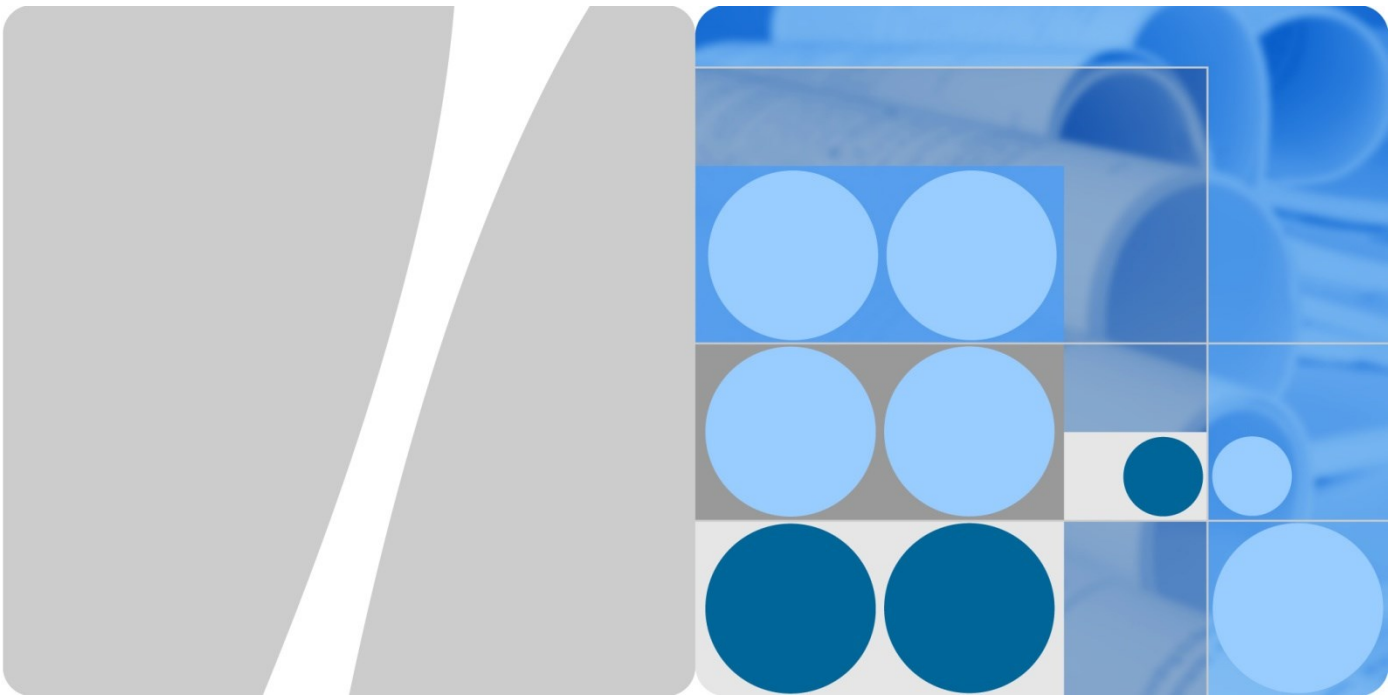


Huawei OptiX OSN 9800 & OptiXtrans E9600 management component software V100R024C10SPC100 - ST

Issue 0.19

Date 2026-10-14

HUAWEI TECHNOLOGIES CO., LTD

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	http://www.huawei.com
Email:	support@huawei.com

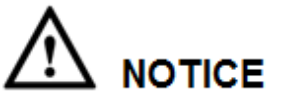
About This Document

Purpose

This Security Target is for the evaluation of OptiX OSN 9800 series (U64E/U32E/M24/M12/M05/P32/P32C) and OptiXtrans E9600 series(E9605/E9612/E9624/E9624X) management component software.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Copyright © Huawei Technologies Co., Ltd.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Date	Version	Change Description	Author
2024-11-07	0.13	Update to R24C10	YangMing
2025-04-21	0.14	Modified TOE's user password length	YangMing
2025-06-07	0.15	Modified TOE's default user password policy	YangMing
2025-11-06	0.16	Update section 6.2.4.2 Change the reference version of CC	YangMing
2026-02-09	0.17	Update section 6.2.2.12,6.2.2.10 and 7.7. Supplemented with DTLS-related content.	YangMing
2026-07-17	0.18	Minor Change	YangJun
2026-10-14	0.19	Update section 1.5.2.3,update References AIS20.	Yuan Tengfei

Copyright © Huawei Technologies Co., Ltd.

content

About This Document ii

1 Introduction 1

1.1 ST Identification 1

1.2 TOE Identification 1

1.3 Product overview 2

1.4 TOE Type and TOE Overview 4

1.5 TOE Description 6

1.5.1 Architectural overview of OSN Series device 6

1.5.2 Scope of Evaluation 14

1.5.3 Summary of Security Features 17

2 CC Conformance Claims 22

2.1 CC Conformance Claim 22

3 Security Problem Definition 23

3.1 Asset 23

3.2 Threats 23

3.2.1 Threats 23

3.2.2 Threats Components 24

3.3 Organizational Security Policies 25

3.4 Assumptions 25

4 Security Objectives 27

4.1 Security Objectives for the TOE 27

4.2 Security Objectives for the Operational Environment 27

4.3 Rationale for Security Objectives 28

5 Extended Components Definition 31

5.1 FCS_RNG Generation of random numbers 31

6 Security Requirements for the TOE 32

6.1 Conventions 32

6.2 Security Functional Requirements 32

6.2.1 Security Audit (FAU) 32

6.2.2 Cryptographic Support (FCS) 34

6.2.3 User Data Protection (FDP) 38

6.2.4 Identification and Authentication (FIA) 40

6.2.5 Security Management (FMT) 42

6.2.6 Protection of the TSF (FPT) 44

6.2.7 TOE access (FTA) 44

6.2.8 Trusted Path/Channels (FTP) 44

Copyright © Huawei Technologies Co., Ltd.

6.3 Security Functional Requirements Rationale 45
6.3.1 Coverage 45
6.3.2 Sufficiency 48
6.3.3 Security Requirements Dependency Rationale 52
6.3.4 Justification for unsupported dependencies 56
6.4 Security Assurance Requirements 56
6.5 Security Assurance Requirements Rationale 56
7 TOE Summary Specification 57
7.1 Authentication 57
7.2 Authorization 59
7.3 Auditing 61
7.4 Communication Security 63
7.5 Traffic Flow Control 66
7.6 Security Management 67
7.7 Cryptographic functions 69
8 Crypto Disclaimer 73
8.1 SSH 73
8.1.1 Cryptographic statement 73
8.2 Transport Security Layer protocol 74
8.2.1 Cryptographic statement 74
8.2.2 Supported TLS cipher suites 76
8.3 Password hashing 76
8.3.1 Cryptographic statement 76
A Abbreviations, Terminology and References 77
A.1 Abbreviations 77
A.2 Terminology 78
A.3 References 78

Copyright © Huawei Technologies Co., Ltd.

1 Introduction

This Security Target is for the evaluation of OptiX OSN 9800 series (U64E/U32E/M24/M12/M05/P32/P32C) and OptiXtrans E9600 series(E9605/E9612/E9624/E9624X) management component software.

Since the name "OptiX OSN 9800 series (U64E/U32E/M24/M12/M05/P32/P32C) and OptiXtrans E9600 series(E9605/E9612/E9624/E9624X)" is long, unless otherwise specified, “OSN Series” is used to represent “OptiX OSN 9800 series (U64E/U32E/M24/M12/M05/P32/P32C) and OptiXtrans E9600 series(E9605/E9612/E9624/E9624X)”.

1.1 ST Identification

Title: Huawei OptiX OSN 9800 & OptiXtrans E9600 management component software V100R024C10SPC100 - ST

Version: 0.19

Date: 2026-10-14

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei OptiX OSN 9800 & OptiXtrans E9600 management component software

Version: V100R024C10SPC100

Developer: Huawei Technologies Co., Ltd.

Running on Hardware Models: OptiX OSN 9800 U64E/U32E/M24/M12/M05/P32/P32C and OptiXtrans E9600 E9605/E9612/E9624/E9624X

VRCSPC versions are defined as follows:

- V version is the version of the software or hardware platform that a product bases.
- R version is released for customer at a specific time. It is a collection of features that is embodied in the form of a product.

Copyright © Huawei Technologies Co., Ltd.

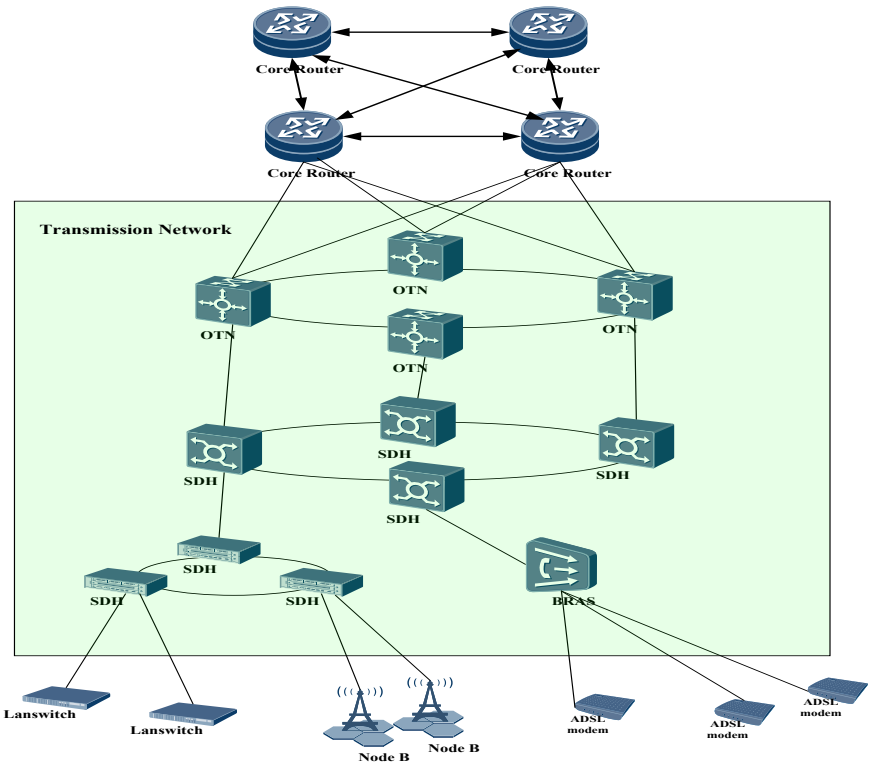
- C version is the customized version developed based on the R version to fast meet customer demands.
- SPC version is the cold service patch version.

The TOE is part of the OSN Series software which is the software running on the OSN Series device.

1.3 Product overview

Transmission networks (including SDH, and WDM/OTN networks) transparently transmit client services from one place to another. For example, as shown in Figure 1-1, Ethernet services are transmitted from LAN (Local Area Network) switch to SDH (Synchronous Digital Hierarchy) equipment, then to OTN equipment, and finally to core routers for routing. During the transmission, transmission equipment encapsulates client services into signals of certain rates, performs error control, and monitors the quality of the signals. To achieve transparent transmission, the transmission equipment does not process client services transmitted from other equipment.

Figure 1-1 Position of the transmission network on the entire communication network



Located at the transmission layer of a communication network, Huawei transmission equipment provides large-capacity and high-reliability transparent transmission tunnels, and is almost invisible to end users.

A Transmission layer of a communication network divide into three layers:

- the edge/access layer of the network,
- the metro/aggregation layer of the network,

Copyright © Huawei Technologies Co., Ltd.

- the backbone/core layer of the network.

The edge/access layer of the network is mainly responsible for the access control of the services of individual and enterprise users. The metro/aggregation layer of the network is to converge the massive user traffic and connect the edge/access layer and backbone/core layer of network. The role of the backbone/core layer of the network is to provide the export of the network, connect with all backbone/core networks, and connect with the Internet Data Center of the city or country. Backbone networks are high-speed networks used to connect multiple regions' networks such as metropolitan area networks or other backbone networks.

The OptiX OSN 9800 & OptiXtrans E9600 is targeted for use at the backbone/core and metro/aggregation layer. It can work with OptiX OSN 1800 to form a complete OTN-based end-to-end network for unified network management as shown in Figure 1-2.

OptiX OSN 9800 and OptiXtrans E9600 are two different commercial brands for different customers. OptiX OSN 9800 is used by both carriers and enterprise networks, and OptiXtrans E9600 is a new commercial brand for enterprise networks.

Intended for 100G and beyond 100G optical networks, the OptiX OSN 9800 U64E/U32E device is a next-generation large-capacity OTN product that integrates ASON, OTN, and packet functions. It is applicable to various networks, including super-backbone and backbone networks.

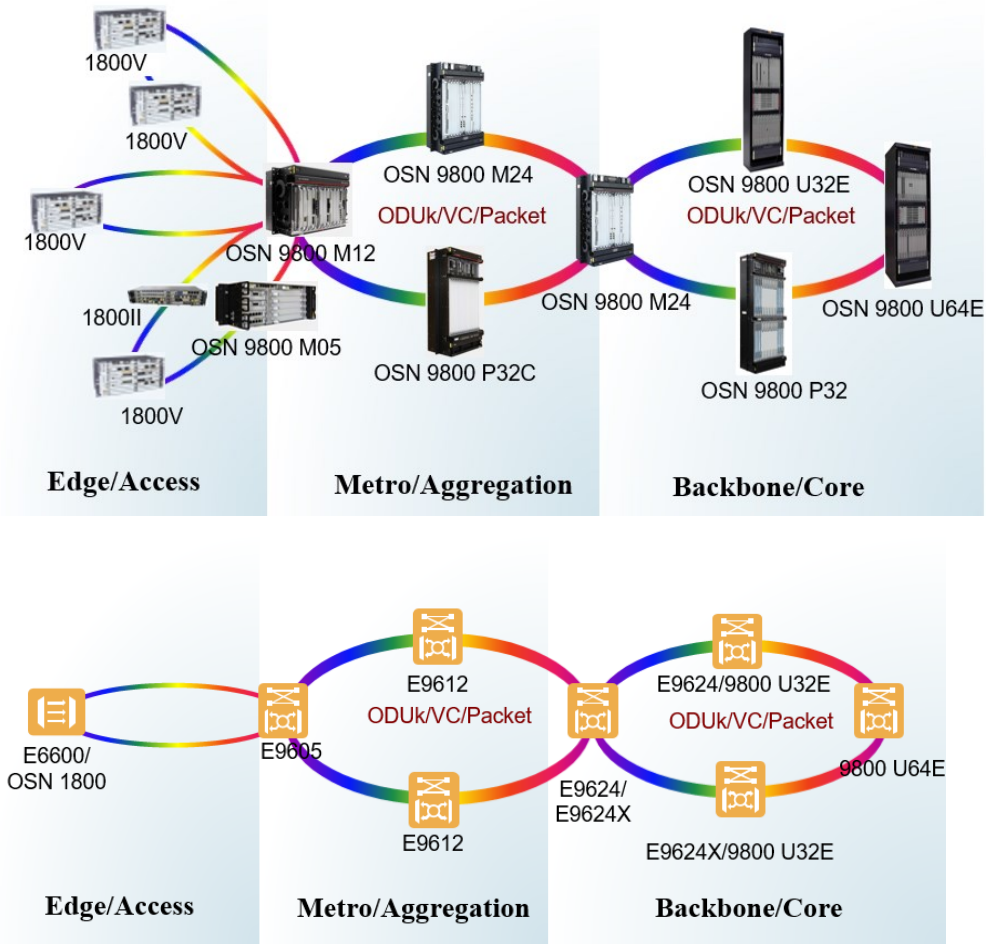
The next-generation OptiX OSN 9800 M series and OptiXtrans E9605/E9612/E9624 devices feature large capacity, optical-electrical integration, and small size. The devices apply to integrated bearing scenarios, such as broadband video, mobile backhaul, enterprise private line, and DCI, and provide an optimal end-to-end transmission solution from the backbone/core layer, metro/aggregation layer, to edge/access layer.

The OptiX OSN 9800 P32/P32C device is an ultra-large capacity all-optical cross-connect product. It is mainly used at the backbone/core layer and metro/aggregation layer. It works with the OSN 9800/1800 to build a complete E2E WDM/OTN backbone transmission solution, achieving transparent and ultra-large capacity transmission.

The OptiXtrans E9624X is an intelligent all-optical transmission platform designed for enterprises. It can be widely used in industries such as electric power and transportation that are crucial to national economy and people's livelihood, guaranteeing that a large amount of production data is securely and reliably transmitted between backbone and metro networks in major cities.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 Position of the OptiX OSN 9800 and OptiXtrans E9600 on the entire network



1.4 TOE Type and TOE Overview

The OSN Series device is transmission equipment and is mainly applicable to the core/backbone and metro/aggregation layer of the network. It is generally deployed in the upstream of wired broadband and mobile carrier facilities, which consists of software and hardware.

The hardware is composed of cabinet, chassis, power unit, and boards. The cabinet is used to install chassis and power units. The power unit is used to supply power to the chassis. The chassis provides the board slot to insert boards.

Boards are the core unit of processing and management in transmission equipment, consisting of SCC (System Control and Communication) unit and service unit. Service unit consisting of OTN board, Optical layer board, Packet board, and TDM board etc.

The SCC (System Control and Communication) unit is the center of the system. All service units are centrally managed and controlled by the SCC unit, in which independent control and management software is running.

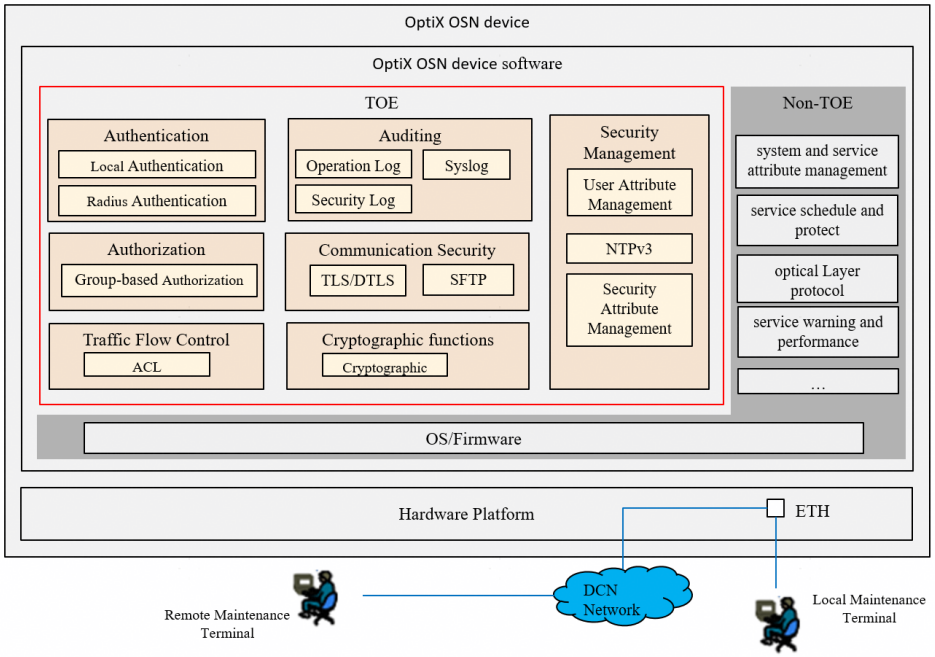
The OSN Series software is deployed in the SCC unit and service units, which is responsible for the system management and control and service transmission.

Copyright © Huawei Technologies Co., Ltd.

The TOE is part of the OSN Series software which contains management component, which is running on the OSN Series device, as shown in Figure 1-3. The TOE is deployed in the SCC unit.

The non-TOE SW components include OS, firmware (the driver software necessary to communicate with the hardware), system and service attribute management, service schedule and protect, optical Layer protocol, and service warning and performance, etc.

Figure 1-3 TOE constitution



To counter the security threats of OSN Series, the TOE deployed in SCC unit provides security measures to mitigate security risks effectively. The main security features are:

1. Authentication
2. Authorization
3. Auditing
4. Communication Security
5. Traffic Flow Control
6. Security management
7. Cryptographic functions

The detailed description of above security features is in the chap.1.5.

1.5 TOE Description

This chapter provides an architectural overview of OSN Series device including a detailed description of the physical architecture and the software architecture, the definition of the TOE subject to evaluation and a summary of security functions provided by the TOE.

Copyright © Huawei Technologies Co., Ltd.

1.5.1 Architectural overview of OSN Series device

This section will introduce OSN Series device from a physical architectural point of view and a software architectural point of view.

1.5.1.1 Physical Architecture

The OSN Series device consists of the hardware and the software.

As shown in Figure 1-4 to Figure 1-11, the hardware is composed of different boards with different board names. CTU, CXP, HCXP, EFI, UCXCS, PIU, APIU, PSU and FAN are the names of different boards.

UCXCS is the universal cluster cross-connect and synchronous timing board, EFI is the external functionality interface board, PIU/APIU is the power interface unit, PSU is the power supply unit, FAN is the fan board.

CTU, CXP and HCXP are the SCC board: CTU is the system control and communication board with clock processing function; CXP/HCXP is the universal cross connect, system control and clock processing board. And all OSN Series devices contain 2 SCC boards.

On the management plane, the two SCC boards work in the active/standby mode. The CPU on the active SCC board manages the system while the CPU on the standby SCC board is in the standby state. The active-standby mode is not a claimed security feature.

The identifier for the SCC boards used in the evaluated configuration of the TOE is listed in Table 1-1. However, the TOE also runs on other SCC boards with the same functionality.

Table 1-1 SCC used in the evaluated configuration

Chassis	**SCC type: slot**	**SCC board Identification**
OptiX OSN 9800 M24 OptiXtrans E9624	CXP: IU71, IU72	TNG4CXP
OptiX OSN 9800 M12/M05 OptiXtrans E9612/ E9605	CTU: IU73, IU74	TME3CTU
OptiX OSN 9800 U32E/ U64E	CTU: IU70, IU78	TNU4CTU
OptiX OSN 9800 P32/ P32C	CTU: IU105, IU107	TMP2CTU
OptiXtrans E9624X	HCXP: IU71, IU72	TNG1HCXP

Copyright © Huawei Technologies Co., Ltd.

Figure 1-4 System architecture of the OptiX OSN 9800 M24/OptiXtrans E9624

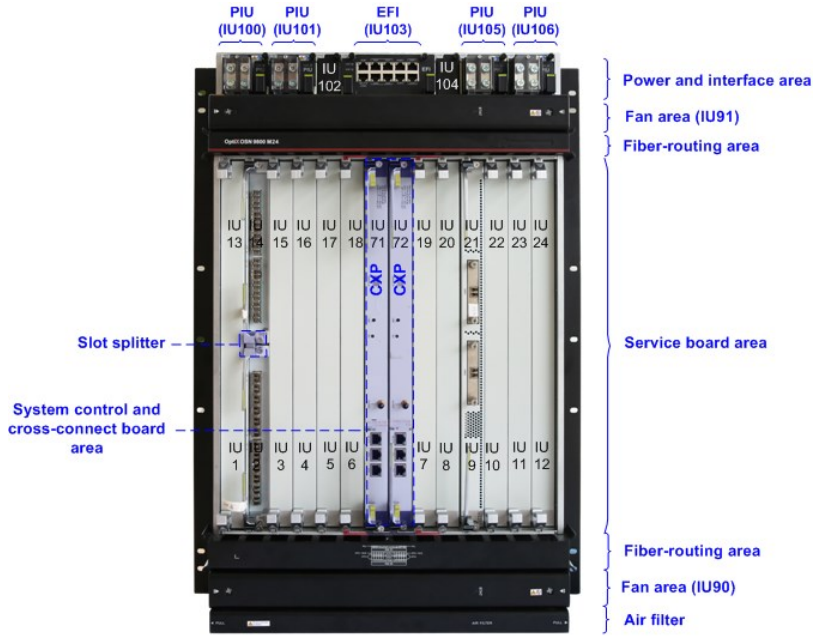
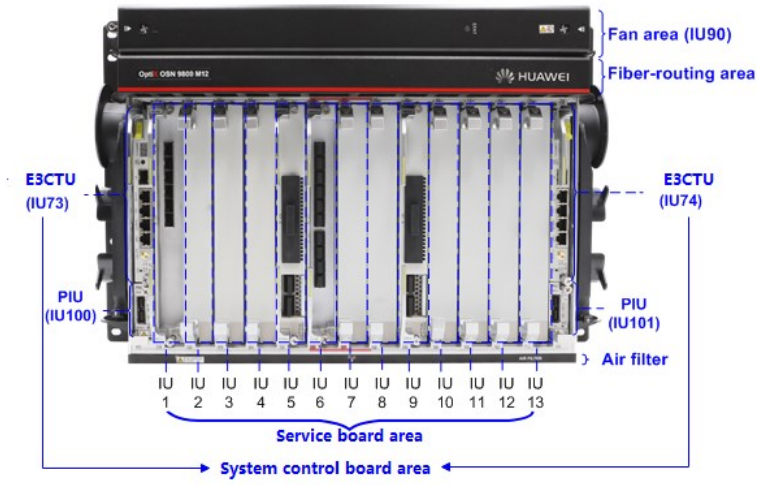
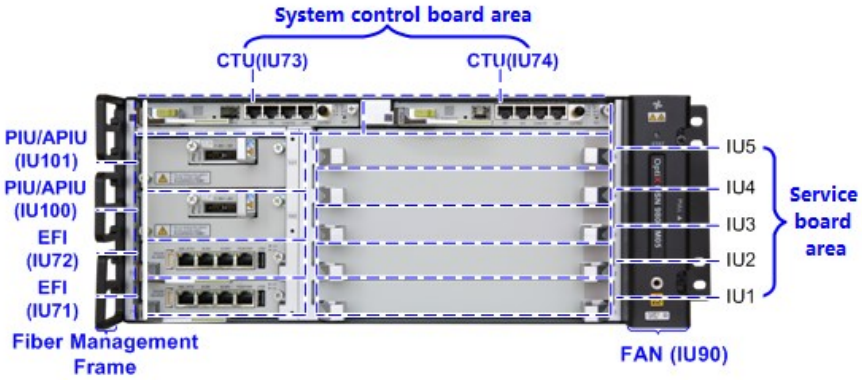


Figure 1-5 System architecture of the OptiX OSN 9800 M12/OptiXtrans E9612



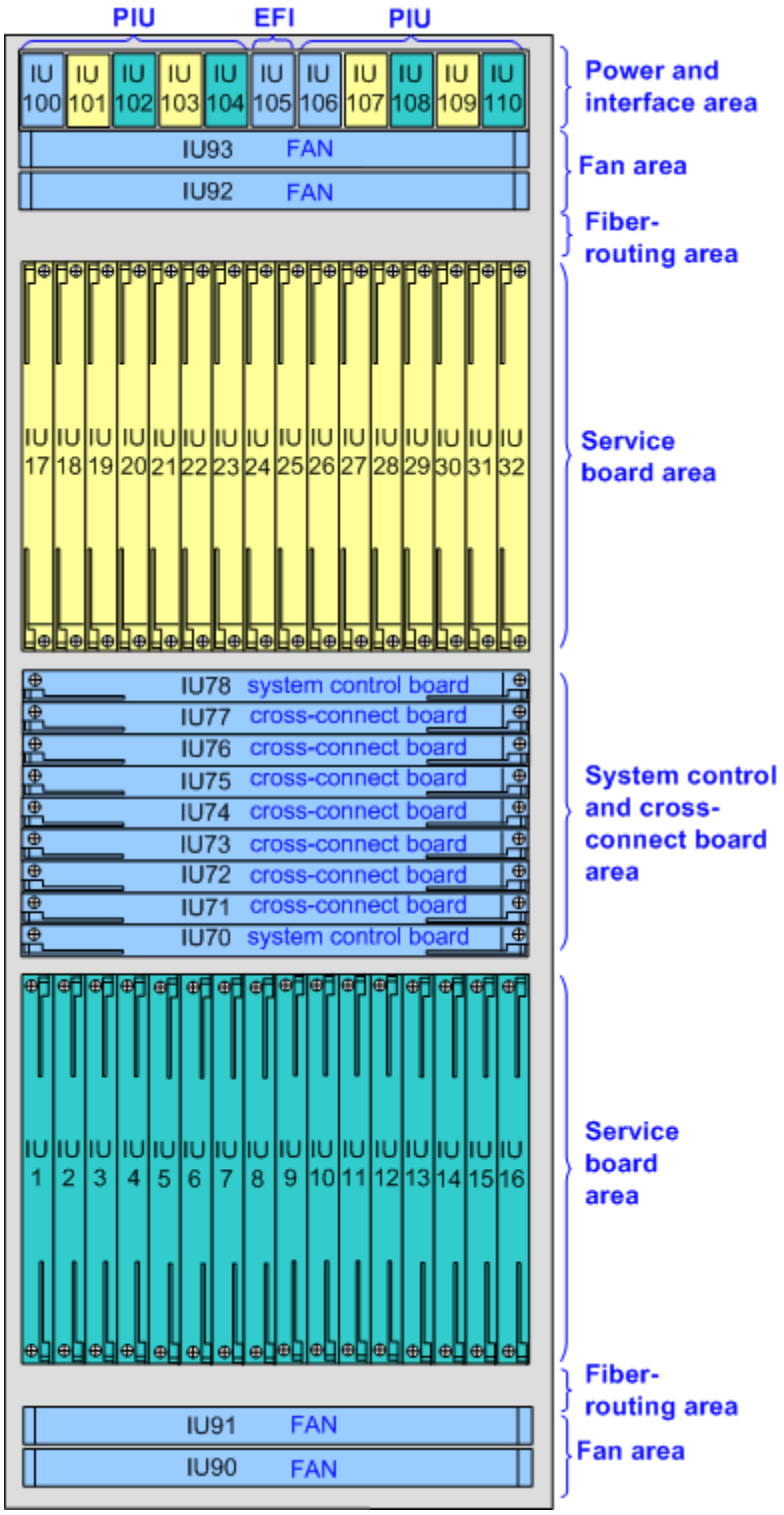
Copyright © Huawei Technologies Co., Ltd.

Figure 1-6 System architecture of the OptiX OSN 9800 M05/OptiXtrans E9605



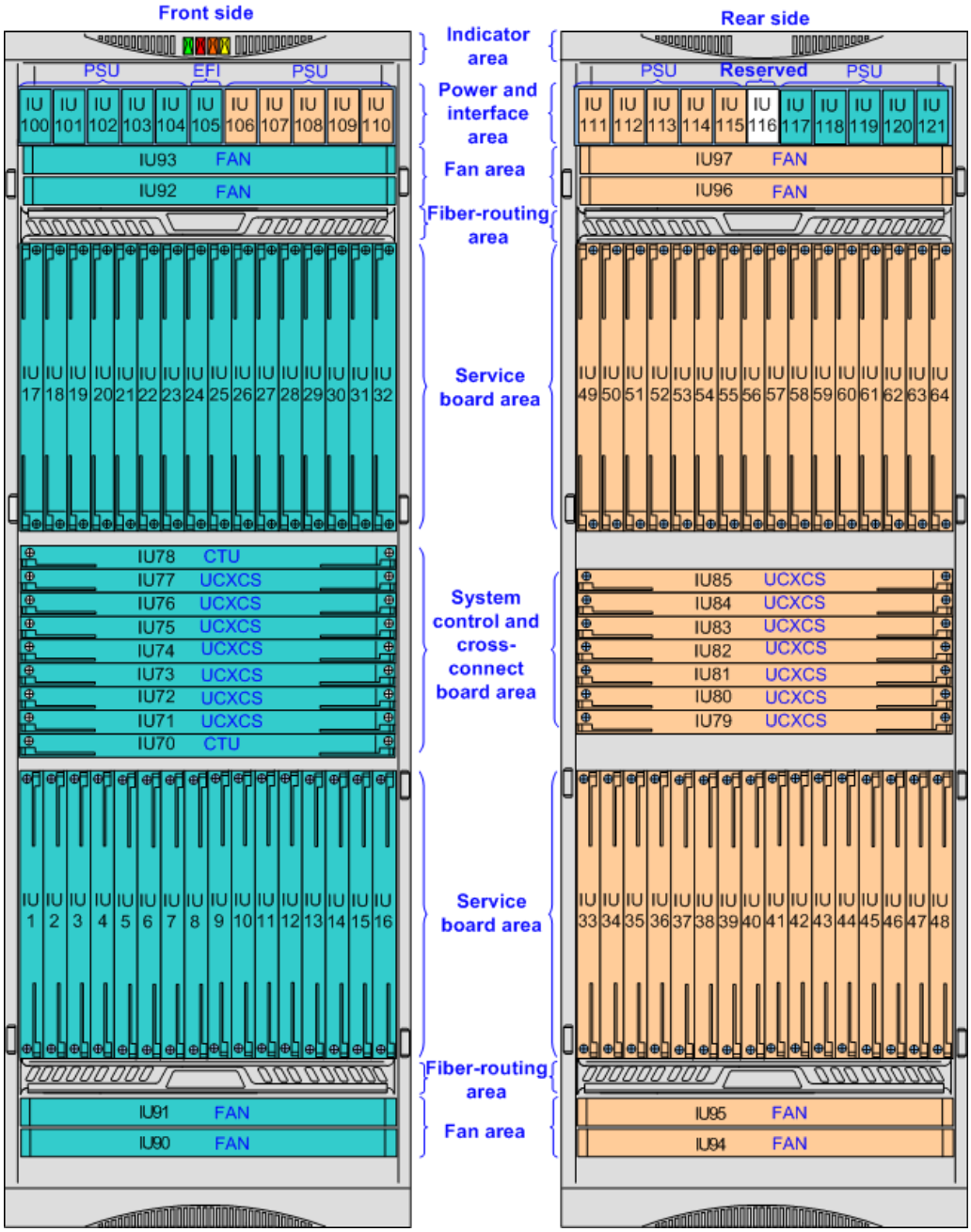
Copyright © Huawei Technologies Co., Ltd.

Figure 1-7 System architecture of the OptiX OSN 9800 U32E



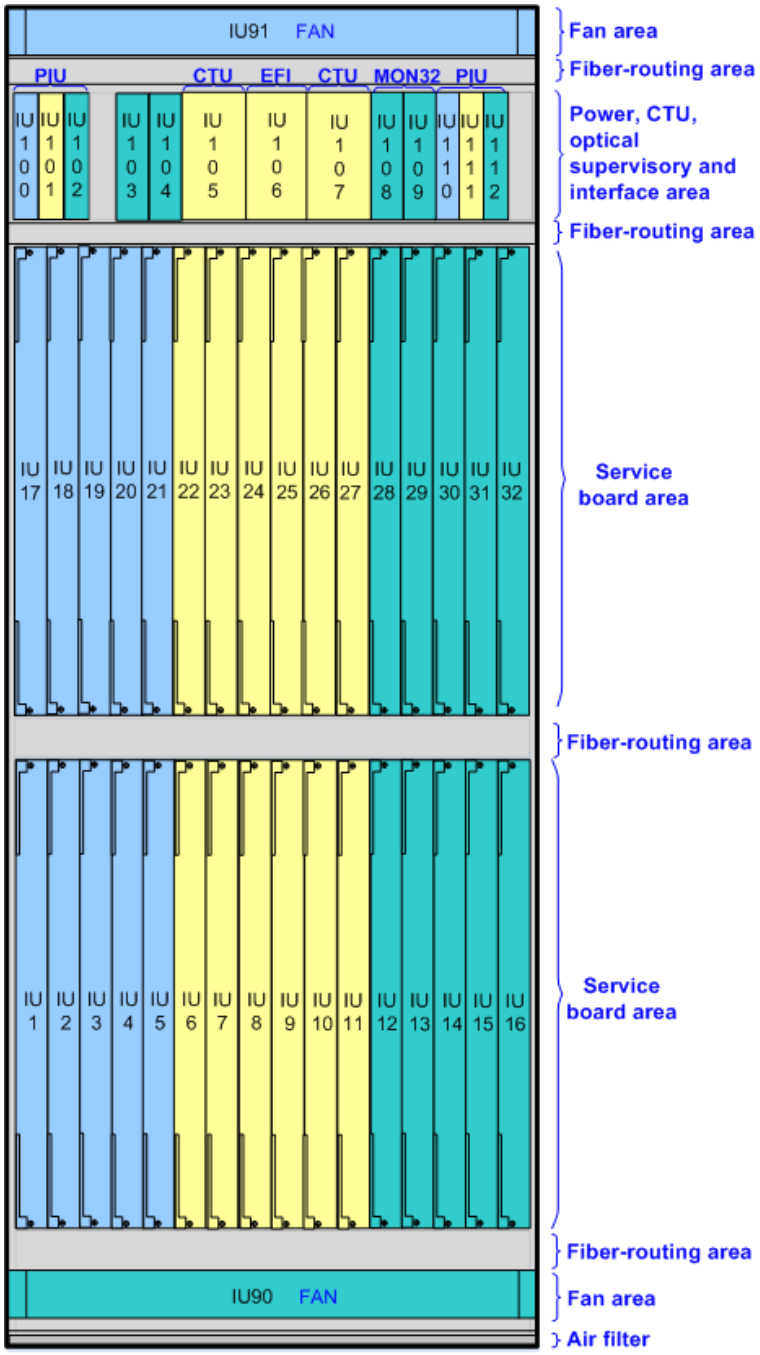
Copyright © Huawei Technologies Co., Ltd.

Figure 1-8 System architecture of the OptiX OSN 9800 U64E



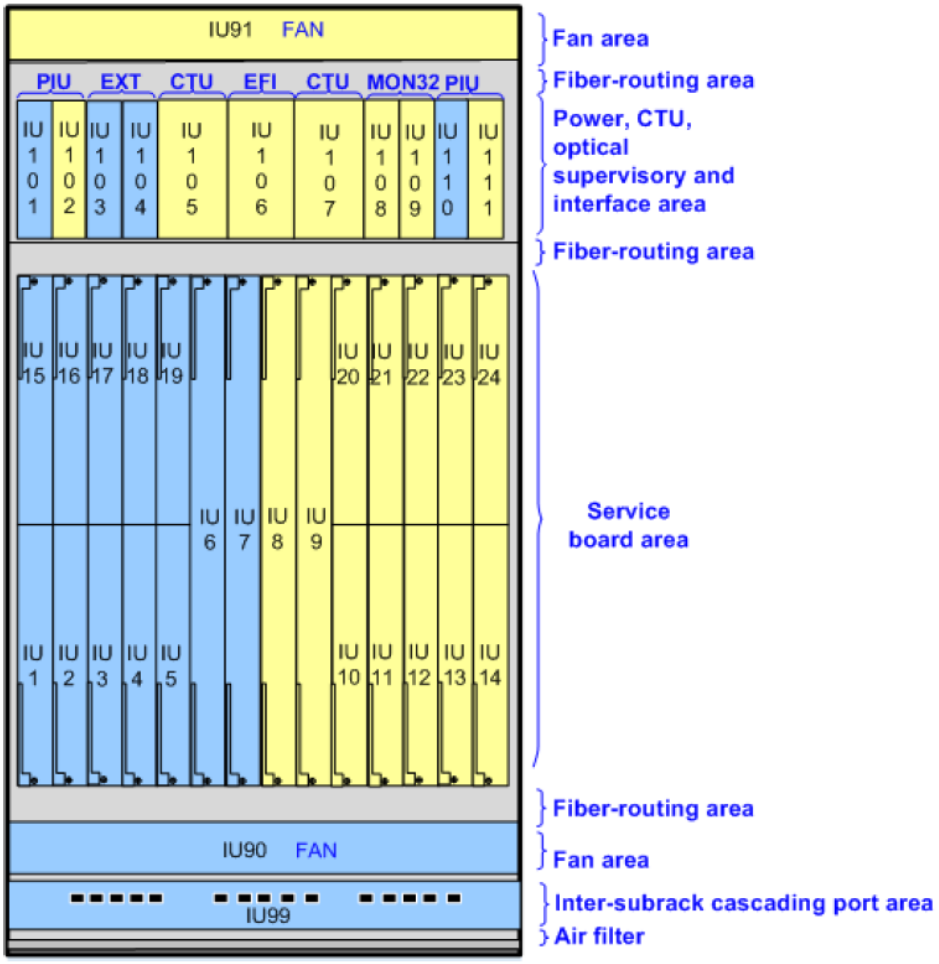
Copyright © Huawei Technologies Co., Ltd.

Figure 1-9 System architecture of the OptiX OSN 9800 P32



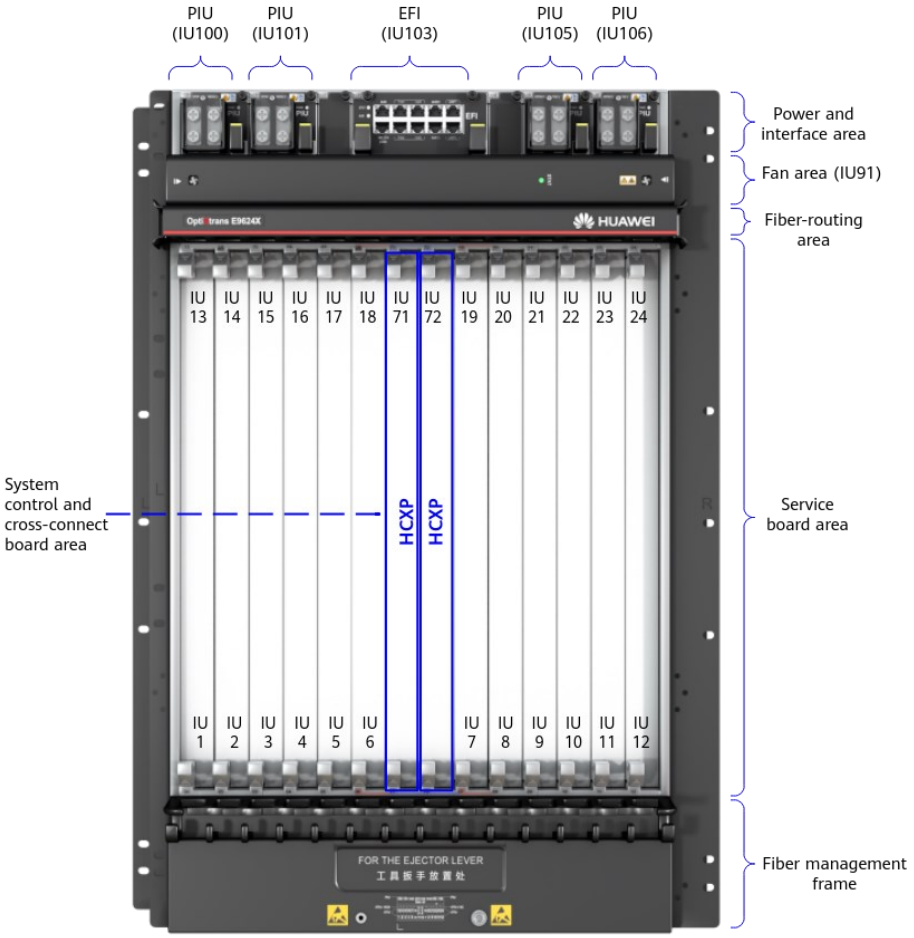
Copyright © Huawei Technologies Co., Ltd.

Figure 1-10 System architecture of the OptiX OSN 9800 P32C



Copyright © Huawei Technologies Co., Ltd.

Figure 1-11 System architecture of the OptiXtrans E9624X



1.5.1.2 Software Architecture

In terms of the software, OSN Series device's software architecture consists of three logical planes to support centralized controlling and management and transparent transmission mechanism:

- Management plane
- Control plane
- Data plane

The **management plane** provides access to the required equipment and management functions, such as managing accounts and passwords, running communication protocols, and reporting alarms.

The **control plane** automatically calculates services paths, and creates and manages services.

The **data plane** is responsible for high speed processing and non-blocking forwarding of data packets. It encapsulates or decapsulates packets, transparently transmits them, and collects statistics.

The TOE only relevant to **management plane**.

Copyright © Huawei Technologies Co., Ltd.

1.5.2 Scope of Evaluation

This section will define the scope of the part of the OSN Series comprising the TOE to be evaluated.

1.5.2.1 Physical scope

The TOE is software only (software package version: V100R024C10SPC100) and is limited to the management component. It is running on the OSN Series devices. The hardware is out of the TOE scope. The devices with pre-installed OSN Series software (not necessary to include the TOE version) are shipped in sealed boxes through worldwide logistics service providers to regional warehouses, from where the devices are delivered to customers efficiently and securely. The following table will define the physical scope of TOE.

Type	Delivery Item	Version
Software	OptiX OSN 9800 U Series(U64E/U32E) Software file: OptiX OSN 9800 E_V100R024C10SPC100.zip Software Signature file: OptiX OSN 9800 E_V100R024C10SPC100.zip.asc	V100R024C10SPC100
	OptiX OSN 9800 M Series(M24/M12/M05) Software file: OptiX OSN 9800 M_V100R024C10SPC100.zip Software Signature file: OptiX OSN 9800 M_V100R024C10SPC100.zip.asc	
	OptiX OSN 9800 P Series (P32/P32C) Software file: OptiX OSN 9800 P_V100R024C10SPC100.zip Software Signature file: OptiX OSN 9800 P_V100R024C10SPC100.zip.asc	
	OptiXtrans E9600 Series (E9605/E9612/E9624/E9624X) Software file: OptiXtrans E9600_V100R024C10SPC100.zip Software Signature file: OptiXtrans E9600_V100R024C10SPC100.zip.asc	
	Info: HUAWEI engineers download the software from support website, and upload the software to the sever provided by the customer. The server information is provided by customers through Email. Users can follow the AGD_OPE document to verify the software by digital signature (The digital signature is also published on HUAWEI support website).	
Product Guidance	Huawei Optix OSN 9800 & OptiXtrans E9600 management component software V100R024C10SPC100 - AGD_OPE Huawei Optix OSN 9800 & OptiXtrans E9600 management component software V100R024C10SPC100 - AGD_PRE Info: The documentation is delivered as a word document.	

Copyright © Huawei Technologies Co., Ltd.

	When transferring files with customers, PGP is used to ensure integrity and authenticity. Customers have their own private keys and Huawei's public keys, and Huawei has their own private keys. When sending a file, you can use Huawei's private key to sign the file, use the customer's public key to encrypt the file, and then send the encrypted file to the customer. After receiving the email, the customer uses the Huawei public key to verify the signature. After the signature passes the signature verification, the customer uses the private key to decrypt the required file to obtain the required file.	
	OptiX OSN 9800 V100R024C10 Product Documentation OptiXtrans E9600 V100R024C10 Product Documentation Info: Users can login the HUAWEI support website to read the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website.	V100R024C10
	OSN 9800 U&M&P&K Series Security Configuration, Maintenance and Hardening Guide OptiXtrans E9600 Series Security Configuration, Maintenance and Hardening Guide Info: Users can login the HUAWEI support website to read the document directly or download the Security Configuration, Maintenance and Hardening Guide in accordance to the version of the TOE. The download file format is *.pdf.	

1.5.2.2 Logical scope

The TOE boundary from a logical point of view is represented by the elements that are displayed with a red frame within the rectangle in Figure 1-3. The TOE is part of the OSN Series software which contains management component. The TOE is running on the eight cores of the CPU. The service unit (including OTN board, Optical layer board, Packet board, and TDM board etc) does not contain parts of the TOE. The TOE provides several security functions, which are described in more detail in chap.1.5.3.

All the security functions claimed in the ST are provided by the TOE.

1.5.2.3 Non-TOE Hardware and Software

The environment for TOE comprises the following components:

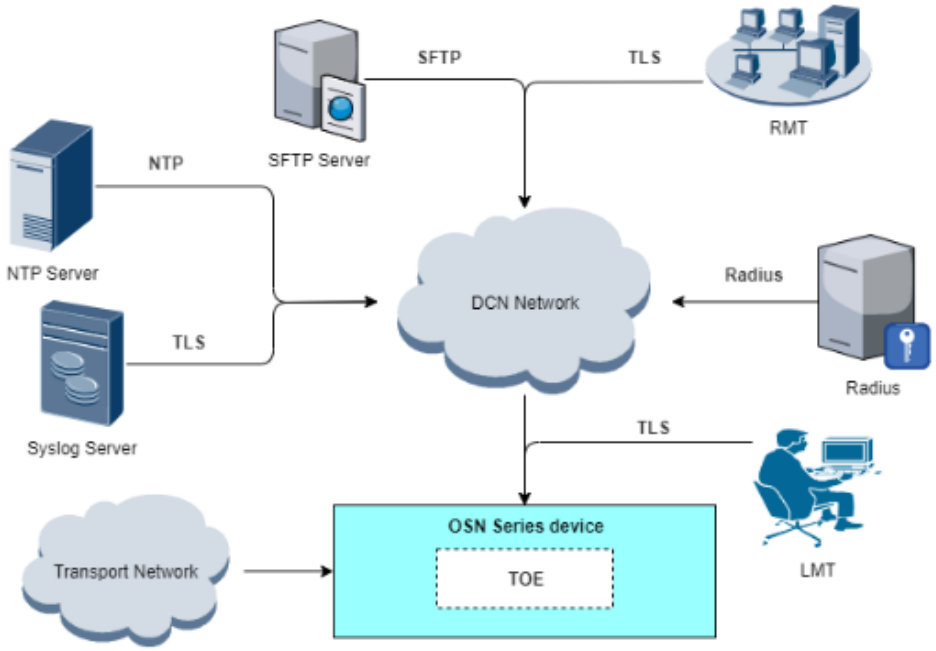
- The LMT/RMT accesses the TOE via the ETH interfaces, and the communication is protected by TLS.
- The LMT is directly connected to the TOE, and the RMT is connected to the TOE through the DCN network. In addition, the tool used by LMT is called WebLCT (the official name is “iMaster NCE Web LCT”), and the tool used by RMT is called NCE (the official name is “iMaster NCE-T”). Both WebLCT and NCE are developped by Huawei. The NCE or WebLCT can be used for commissioning and configuration during site deployment. All functions supported by the WebLCT are available on the NCE. However, the WebLCT is less demanding on computer hardware and its startup process takes less time. Generally,

Copyright © Huawei Technologies Co., Ltd.

the WebLCT is recommended for commissioning a site locally and the NCE is recommended for remote commissioning performed at the network operation center.

- Since the TOE is part of the OSN Series device as shown in Figure 1-3, and it can only operate as part of the device, which means that all non-TOE parts of the device are also required. The OSN Series hardware and non-TOE software are therefore part of the operational environment.
- Furthermore, the TOE may use a Radius server, a Syslog server, and an NTP server, and requires an SFTP (FTP over SSH) server, as shown in the following figure. A Radius server is optional and may be used instead of local authentication. A Syslog server is optional if you want to upload log to log server, and an NTP server is optional and may be used instead of manual configuration. An SFTP server is mandatory and is used for secure file transfer during upgrade.

Figure 1-12 The TOE in its operational environment



1.5.3 Summary of Security Features

1.5.3.1 Authentication

Authentication is the process wherein the system checks the validity of accounts and passwords. All users that are connected must be authenticated and then they can operate the TOE.

The TOE provides a local authentication mode, or can optionally enforce authentication decisions obtained from a Radius server in the IT environment.

In local authentication mode, accounts and passwords are saved on the local equipment and authenticated using the local account and password by the local equipment during login. In RADIUS authentication mode, accounts and passwords are saved on the RADIUS server and authenticated by the RADIUS server. During login, the accounts and passwords are forwarded

Copyright © Huawei Technologies Co., Ltd.

to the RADIUS server, using the RADIUS protocol and the RADIUS server checks the validity of accounts and passwords.

User authentication is always enforced for RMT/LMT. The use of TLS connection is always required for accessing the TOE via RMT/LMT.

1.5.3.2 Authorization

Authorization indicates that devices assign operation authorities to accounts according to their validity.

The TOE controls access by the group-based authorization framework with predefined role groups for management. Four hierarchical access groups are offered and can be assigned to individual user accounts.

Only authenticated users can execute operate of the TOE. Only one user group level can be assigned to a user account. So the user group level of a user is unambiguous at any time.

Accounts are managed in groups and each group represents a specific authority assigned to the accounts in the group. Table 1-2 lists the groups and their definition. For example, the accounts of the "Administrator" group are authorized to perform all security management and advanced diagnosis operations. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account attempts to perform any unauthorized operation, an error message is displayed and the attempt is logged.

Table 1-2 Groups of accounts

Group	Authority
Monitor	This group has the lowest authority. The accounts of this group are authorized to issue query commands and modify some of their own attributes.
Operator	The accounts of this group are authorized to query the system information and perform some configuration operations.
Maintenance	The accounts of this group are authorized to perform all maintenance operations, including the authority of Operator group and general maintenance and diagnosis operations
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations. Especially, Administrators are also authorized to perform the advanced diagnosis (debug) operation.

Note: user level in the following content is same as user group; in CC terminology, these are considered roles.

1.5.3.3 Auditing

Logs record routine maintenance events of the TOE. Administrators can find security vulnerabilities and risks by checking logs. Considering security, the TOE provides security logs and operation logs.

Security logs record operation events related to account management, such as modification of passwords and addition of accounts.

Copyright © Huawei Technologies Co., Ltd.

Operation logs record events related to system configurations, such as modification of equipment IP addresses and addition of services.

The TOE provides a Syslog solution to resolve the problem of limited equipment storage space. Both security logs and operation logs can be saved on an external Syslog server.

1.5.3.4 Communication Security

The TOE provides communication security by implementing the TLS/DTLS protocol and the SFTP protocol for different use cases.

For the secure communication between the TOE and the RMT/LMT/Syslog server the TLS protocol is used. TLS version 1.2 and 1.3 are implemented. TLS certificates are required for establishing TLS encryption channels. The TLS certificates are managed and issued by the user of the TOE (mainly Internet Service Providers ('carriers')). The TOE acts as server during the TLS communication established between the TOE and RMT/LMT, while it acts as client during the TLS communication with the Syslog server.

The TOE uses the DTLS protocol to provide secure communication between the TOE and the RADIUS server. The secure communication between the TOE and the RADIUS server uses DTLS certificates to establish DTLS encrypted channels. Certificates are managed and issued by TOE users. Before establishing DTLS communication, the certificates are loaded to TOE using SFTP.

TLS (RFC 5246 / RFC 8446) and DTLS (RFC 6347) share the same security architecture, including handshake mechanisms, key derivation processes, cipher suite structure and security objectives.

Therefore, unless explicitly stated otherwise, the description of the protocol mechanisms (e.g., handshake steps, key derivation, cryptographic algorithms, certificate processing, and session protection properties) applies equally to TLS and DTLS.

The only differences relevant to the TOE are:

The TOE supports TLS 1.2 and TLS 1.3, while DTLS is supported in version 1.2 only.

The exact cipher suites available for TLS and DTLS may differ slightly and are listed separately in the FCS and TOE Summary Specification.

To avoid unnecessary duplication, the ST describes the protocol mechanisms in a unified way, and differences between TLS and DTLS are highlighted only when relevant (such as version support or cipher suite specification).

The TOE provides an SFTP client for secure file downloading and uploading. Users can use the SFTP client for fault collection, log uploading, and uploading and downloading of a file and a database etc. In this application, the TOE serves as a client and the SFTP server is deployed outside the equipment network and is provided by the carrier.

The SFTP authentication policy is determined by the SFTP server. The TOE supports password authentication and key authentication. The password authentication indicates that an SFTP client logs in to a server using an account name and a password. The key authentication indicates that an SFTP server authenticates a client using the ED25519 key. For the key authentication, users need to generate the ED25519 key on the TOE first and upload the public key to the SFTP server. The length of the ED25519 key is 256 bits.

The TOE uses passphrases to protect private keys on an SFTP client for cryptographic authentication. When users generate key pairs, they are allowed to indicate the passphrases.

Copyright © Huawei Technologies Co., Ltd.

1.5.3.5 Traffic Flow Control

For administration of the TOE, network packages have to be sent to the TOE from the management network. The TOE provides Access Control List (ACL) for filtering incoming information flows to management interfaces in Table 1-3. An Administrator can set deny IP addresses and ports, to limit data from specific IP addresses and to filter data from specific communication ports. The ACL function protects equipment from network attacks by controlling data of access requests from unauthorized IP addresses and ports. The Administrator can create, delete, and modify ACL rules in Table 1-4. Packet flows matching a deny rule in the ACL are dropped. If no rule is specified for an incoming packet, it is accepted by default.

The "management interfaces" is "ETH interfaces", "ETH interfaces" are dedicated to the TOE management, and all devices (RMT/LMT/SFTP/RADIUS/SYSLOG/NTP) are connected to the TOE through ETH interfaces. All traffic passing through the ETH interfaces is filtered.

Table 1-3 Classification of ACL

Item	Feature
Basic ACL	Rules are defined based on the source IP address.
Advanced ACL	Rules are defined based on the source IP address of a data packet, destination IP address of a data packet, protocol type of the IP bearer network, and protocol features, etc. For details, refer to Table 1-4.

Table 1-4 ACL parameters

Parameter	Value Range	Description
ACL rule ID	0–0xFFFFFFFF	Indicates the ACL rule ID. The value 0xFFFFFFFF indicates that the ACL rule is automatically allocated by the ACL protocol or is manually assigned.
ACL operation type	Permit and deny	Indicates the ACL operation type. The values are as follows: • Deny: If a received message matches a deny rule in an ACL, the message is discarded. • Permit: If a received message matches a permit rule in an ACL, the message is forwarded.
Source IP address	Source IP address	The source IP address and the source wildcard determine the addresses to which an access control rule is applicable.
Source wildcard	0–0xFFFFFFFF	The value 0 represents a bit that must be exactly matched and the value 1 represents a bit that is ignored.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value Range	Description
Destination IP address	Destination IP address	The destination IP address and the destination wildcard determine the addresses to which an access control rule is applicable.
Destination wildcard	0–0xFFFFFFFF	The value 0 represents a bit that must be exactly matched and the value 1 represents a bit that is ignored.
Protocol type	TCP, UDP, ICMP, and IP	Set this parameter to UDP or TCP when filtering packets at a UDP or a TCP port. Set this parameter to ICMP when filtering packets of the ICMP protocol and code type. The value IP indicates that the protocol type is not concerned.
Source port	0–65535 or 0xFFFFFFFF (0xFFFFFFFF indicates that this parameter is not concerned)	This parameter is available only when **Protocol type** is set to **TCP** or **UDP**.
Destination port	0–65535 or 0xFFFFFFFF (0xFFFFFFFF indicates that this parameter is not concerned)	This parameter is available only when **Protocol type** is set to **TCP** or **UDP**.
ICMP protocol type	ICMP protocol type	This parameter is available only when **Protocol type** is set to **ICMP**. The value 255 indicates that this parameter is not concerned.
ICMP code type	ICMP code type	This parameter is available only when **Protocol type** is set to **ICMP**. The value 255 indicates that this parameter is not concerned.

1.5.3.6 Security management

Security functionality management include not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

The functions mainly include:

- Management of user accounts and user attributes, including user credentials.
- Management of authentication failure policy
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces
- Management of ACLs and ACL attributes and parameters like IP addresses or address ranges

Copyright © Huawei Technologies Co., Ltd.

- Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP
- Management of the TOE's time

All security management functions (i.e. commands related to security management) require sufficient user group for execution (see description of access control for details, chap. 1.5.3.2).

Copyright © Huawei Technologies Co., Ltd.

1.5.3.7 Cryptographic functions

The TOE does not offer cryptographic services, but uses cryptographic mechanisms in the implementation of its communication security functions (TLS, SFTP) and I&A functions (certificates, SFTP public key authentication).

Details of the algorithms, key lengths and modes of operation are provided in section 7.7 .

2 CC Conformance Claims

2.1 CC Conformance Claim

This ST is *CC Part 2 extended* [CC], extended by security functional components as defined in chap. 5, and *CC Part 3 conformant* [CC]. The version of [CC] is 3.1R5.

The ST claims conformance to the EAL3 augmented with ALC_FLR.2.

No conformance to a Protection Profile is claimed.

Copyright © Huawei Technologies Co., Ltd.

3 Security Problem Definition

3.1 Asset

The assets to be protected are the information stored, processed or generated by the TOE. Including below:

1. Audit data: The data which is provided by the TOE during security audit logging
2. Authentication data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
3. Crypto data: All data used by the TOE for cryptographic operations like digital signature handling and encryption or decryption purposes. This includes symmetric and asymmetric cryptographic keys.
4. Configuration data: The data for the TOE, which is used for configuration of security feature and functions. This includes also data which is used by the TOE for system software, patches update, and identity checking purposes.
5. Management Traffic data, which is the management information exchanged between the TOE and the RMT/LMT from authorized users and between the TOE and the SFTP server.

3.2 Threats

This section specifies the threats that are addressed by the TOE and the TOE environment.

As a result, the following threats have been identified:

3.2.1 Threats

T.UnwantedManagementTraffic The traffic here only refers to the traffic on management interfaces, that means, the Unwanted Network Traffic threat only exists on the management plane. The Unwanted network traffic may originate from an attacker and result in an overload of the management interfaces, which may cause a failure of the TOE to respond to system control and normal management operations. As a consequence, the TOE might be unable to provide some of the TSF while under attack and in particular security management functionality to update configuration data for the TOE. Subsequently, backup of audit information before local storage space is exceeded and old audit information is overwritten by

Copyright © Huawei Technologies Co., Ltd.

new audit events could be affected. Therefore, Audit data and Configuration data for the TOE are assets that could be affected by this threat, too.

T.UnauthenticatedAccess An unauthenticated person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE. This could affect all assets as defined in chap. 3.1 .

T.UnauthorizedAccess A user with restricted action and information access authorization gains access to unauthorized commands or information. This threat also includes data leakage to non-intended person or device. This could affect all assets as defined in chap. 3.1 .

T.Intercept An attacker is able to intercept, modify and re-use management information assets that are exchanged between the TOE and RMT/LMT and between the TOE and the SFTP server. This comprises Authentication data (in particular authentication data of users), Crypto data (regarding this threat mainly data related to session keys used for secure communication), and Configuration Data for the TOE. In addition, an attacker is able to intercept and modify audit data that is transmitted to the external Syslog server. All these assets could be affected by this threat.

3.2.2 Threats Components

- T.UnwantedManagementTraffic

  Threat agent: Attacker.

  Asset: Audit data, Configuration data.

  Adverse action: Disturbance on TOE operation.

- T.UnauthenticatedAccess

  Threat agent: Unauthenticated person.

  Asset: Authentication data, Audit data, Configuration data, Crypto data, Management Traffic data.

  Adverse action: Access to the TOE.

- T.UnauthorizedAccess

  Threat agent: User with restricted action and information access authorization.

  Asset: Authentication data, Audit data, Configuration data, Crypto data, Management Traffic data.

  Adverse action: perform unauthorized actions and unauthorized access to TOE information and configuration data.

- T.Intercept

  Threat agent: Attacker in the management network.

  Asset: Authentication data, Audit data, Crypto data, Configuration data.

  Adverse action: Intercept, and potentially modify or re-use information that are exchanged between TOE and RMT/LMT and between the TOE and the SFTP/SYSLOG server.

Copyright © Huawei Technologies Co., Ltd.

3.3 Organizational Security Policies

This section specifies one organizational security policy (OSP) to be met by the TOE and the TOE environment.

OSP.Accountability The users of the TOE shall be held accountable for their security-relevant actions within the TOE.

OSP.PasswordHash User passwords shall be hashed in a secure way before being stored in the local storage of the TOE.

3.4 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

A.TLSKeyandCertificate It is assumed that the asymmetric keys for TLS end point authentication are generated in a secure way and are of good quality, i.e. meeting relevant standards and providing sufficient security strength. The corresponding certificates are obtained from trusted certification authorities by secure means and the certificates are of good quality, i.e. the cryptographic mechanisms and parameters used to sign the certificate meeting relevant standards and providing sufficient security strength. It is also assumed that Administrators validate the complete certificate chain and examine the quality of the certificates before importing them. Especially the Administrators check the hash algorithm used to sign the certificate and do not import certificates signed with weak hashing algorithms. The private keys are imported into the TOE in a secure way.

A.PhysicalProtection It is assumed that the TOE and its operational environment (i.e. the complete system including the device hardware and attached peripherals) are protected against unauthorized physical access. It is assumed that only users with explicit approval by the Administrator(s) are authorized to physically access the TOE and its operational environment. This assumption includes the RADIUS server and NTP server together with all related communication lines are operated in the same physically secured environment as the TOE. For LMT, RMT, Syslog server and SFTP server, this assumption only includes the device itself.

A.NetworkElements It is assumed that the operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with. This applies e.g. to the LMTs and RMTs used for TOE management, Syslog servers, SFTP servers and Radius servers for obtaining authentication and authorization decisions. NTP servers for synchronizing time to the TOE.

A.NetworkSegregation It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.

A.NoEvil It is assumed that personnel working as authorized users shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These users are assumed being administration professionals, work not careless or willfully negligent or hostile, and will follow and abide the TOE documentation.

A.Device It is assumed that the underlying hardware of OSN Series, which is outside the scope of the TOE, as well as the non-TOE software, work correctly and do not tamper with the TOE in any manner.

Copyright © Huawei Technologies Co., Ltd.

A.RNG It is assumed that the TPM, which provides the seed to the RNG, is reliable and therefore provides a seed value of sufficient entropy.

A.Time It is assumed that the external clock provided by the NTP server is reliable.

Copyright © Huawei Technologies Co., Ltd.

4 Security Objectives

4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

- **O.DataFilter** The TOE shall ensure that only allowed management traffic goes through the TOE.
- **O.Authorization** The TOE shall implement different authorization roles that can be assigned to users in order to restrict the functionality that is available to them.
- **O.Authentication** The TOE shall authenticate users before access to data and security functions is granted.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrative actions and user log in and log out activities.
- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT as well as between the TOE and trusted IT products, including Syslog/SFTP server, from the operational environment.
- **O.SecurityManagement** The TOE shall provide functionality to manage security functions provided by the TOE.
- **O.PasswordHash** The TOE shall hash user passwords in a secure way before they are stored in the local storage.

4.2 Security Objectives for the Operational Environment

- **OE.TLSKeyandCertificate** The asymmetric keys for TLS end point authentication shall be generated in a secure way and shall be of good quality, i.e. meeting relevant standards and providing sufficient security strength. The corresponding certificates shall be obtained from trusted certification authorities by secure means and the certificates shall be of good quality, i.e. the cryptographic mechanisms and parameters used to sign the certificate meeting relevant standards and providing sufficient security strength. Administrators shall validate the complete certificate chain and examine the quality of the certificates before importing them. Especially the Administrators shall check the hash algorithm used to sign the certificate and shall not import certificates signed with weak hashing algorithms. The private keys areimported into the TOE in a secure way.
- **OE.PhysicalProtection** The TOE and its operational environment (i.e. the complete system including the device hardware and attached peripherals) shall be protected against unauthorized physical access. Only users with explicit approval by the

Copyright © Huawei Technologies Co., Ltd.

Administrator(s) shall be authorized to physically access the TOE and its operational environment. The RADIUS server and NTP server together with all related communication lines shall be operated in the same physically secured environment as the TOE. For LMT, RMT, Syslog server and SFTP server, the device itself shall be physically protected.

- **OE.NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. The behavior of such network devices provided by the operational environment shall be secure and correct. This applies e.g. to LMTs and RMTs used for TOE management, Syslog servers, SFTP servers and Radius servers for obtaining authentication and authorization decisions. NTP servers for synchronizing time to the TOE.
- **OE.NetworkSegregation** The operational environment shall provide segregation of networks by deploying the management interface in TOE into an independent local network.
- **OE.NoEvil** Personnel working as authorized users shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These users shall be administration professionals, work not careless or willfully negligent or hostile, and shall follow and abide the TOE documentation.
- **OE.Device** The underlying hardware of OSN Series, which is outside the scope of the TOE, as well as the non-TOE software, shall work correctly and shall not tamper with the TOE in any manner.
- **OE.RNG** The TPM, which provides the seed to the RNG, shall be reliable and therefore provides a seed value of sufficient entropy.
- **OE.Time** The external clock provided by the NTP server shall be reliable.

4.3 Rationale for Security Objectives

The following table provides a mapping of TOE objectives to threats, showing that each objective is at least covered by one threat in Table 4-1.

Table 4-1 Mapping objectives to threats and OSPs

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.UnwantedManagementTraffic	O.DataFilter O.SecurityManagement	This threat is countered by O.DataFilter ensuring that unwanted traffic is filtered and cannot deplete the network resources. The filter rules can be configured by authorized users with sufficient user group (O.SecurityManagement).
T.UnauthenticatedAccess	O.Authentication O.Audit O.SecurityManagement	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). Authentication mechanisms can be configured by users with sufficient user group (O.SecurityManagement). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).

Copyright © Huawei Technologies Co., Ltd.

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.UnauthorizedAccess	O.Authorization O.Audit O.SecurityManagement	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). Access control mechanisms (including user groups) can be configured by users with sufficient user group (O.SecurityManagement). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).
T.Intercept	O.Communication O.SecurityManagement	The threat of eavesdropping is countered by requiring communications security via TLS for communication between RMT/LMT/Syslog server and the TOE and DTLS for communication between the TOE and the RADIUS server and SFTP for communication between the TOE and the SFTP server (O.Communication). Management of secure communication channels can be performed by users with sufficient user group (O.SecurityManagement).
OSP.Accountability	O.Authentication O.Audit	Accountability for security-relevant actions is achieved by generating audit records for those events (O.Audit). Attributing security-relevant events to their originators requires users to be properly identified and authenticated (O.Authentication)
OSP.PasswordHash	O.PasswordHash	This OSP is enforced by hashing user passwords in a secure way before they are stored in the local storage of the TOE (O.PasswordHash)

The following table provides a mapping of the objectives for the operational environment to assumptions, showing that each objective is covered exactly by one assumption. The objectives for the environment are mirrored by the assumptions. Therefore, the mapping is trivial in Table 4-2.

A.TLSKeyandCertificate is upheld by OE.TLSKeyandCertificate, which is a rephrasing of the assumption.

A.PhysicalProtection is upheld by OE.PhysicalProtection, which is a rephrasing of the assumption.

A.NetworkElements is upheld by OE.NetworkElements, which is a rephrasing of the assumption.

Copyright © Huawei Technologies Co., Ltd.

A.NetworkSegregation is upheld by OE.NetworkSegregation, which is a rephrasing of the assumption.

A.NoEvil is upheld by OE.NoEvil, which is a rephrasing of the assumption.

A.Device is upheld by OE.Device, which is a rephrasing of the assumption.

A.RNG is upheld by OE.RNG, which is a rephrasing of the assumption.

A.Time is upheld by OE.Time, which is a rephrasing of the assumption.

Table 4-2 Mapping objectives for the environment to assumptions

Environmental Objective	**Threat /Assumption**
OE.TLSKeyandCertificate	A.TLSKeyandCertificate
OE.PhysicalProtection	A.PhysicalProtection
OE.NetworkElements	A.NetworkElements
OE.NetworkSegregation	A.NetworkSegregation
OE.NoEvil	A.NoEvil
OE.Device	A.Device
OE.RNG	A.RNG
OE.Time	A.Time

Copyright © Huawei Technologies Co., Ltd.

5 Extended Components Definition

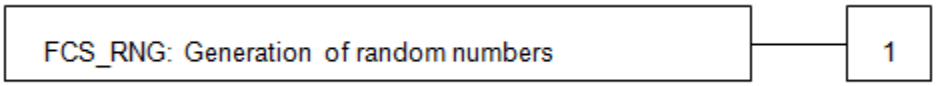
There is one extended component defined which refers to random number generation and is taken from chap. 3.1 [AIS20].

5.1 FCS_RNG Generation of random numbers

Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:



FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Copyright © Huawei Technologies Co., Ltd.

6 Security Requirements for the TOE

6.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- underlined text indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/Identifier distinguishes different iterations.

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) **The following auditable events recorded to operation logs:**

i. user activity

1. **login, logout**
2. **system and service configuration operation requests (i.e. configuration of the device after start-up)**
3. **system security configuration.**

The following auditable events recorded to security logs:

Copyright © Huawei Technologies Co., Ltd.

ii. **user management**

1. **add, delete, modify users**
2. **user password change**
3. **user group level change**
4. **user lock and unlock**

Application Note: Audit functionality shall be enabled by default during start-up of the device. The audit functionality cannot be shut down manually. The audit functionality can only be shut down by shutdown of the OSN Series itself. In that case there is only an audit record generated for the shutdown of the device but not the audit functionality in particular.

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 ST, **Operation Type (if applicable)**, **Operation Object (if applicable), Access IP Address (if applicable)**, **Username (if applicable).**

6.2.1.2 FAU_GEN.2 User Identity Association

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

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **Administrators** with the capability to read **all information** from the audit records.

Application Note: Administrators here refer to the Administrator account group. Monitor, Operator and Maintenance account groups do not have the authority to read audit records.

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

6.2.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.5 FAU_STG.1 Protected Audit Trail Storage

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

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

6.2.1.6 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall **overwrite the oldest records** if the audit trail exceeds **the size of the storage device**.

Application Note: The audit trail is recorded in log file on the storage media (FLASH), the size of log file is fixed.

Copyright © Huawei Technologies Co., Ltd.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1/DH Cryptographic key generation

FCS_CKM.1.1/DH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **FFC schemes** and specified cryptographic key sizes **3072 bits and 4096 bits** that meet the following: **[FIPS 186-4], Appendix B.1.**

Application Note: The TOE generates DH private and public value that are used in TLS key exchanges.

6.2.2.2 FCS_CKM.1/ECDH Cryptographic key generation

FCS_CKM.1.1/ECDH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECC schemes using NIST curves P-256, P-384, P-521 and X25519, X448** that meet the following: **[FIPS 186-4], Appendix B.4 and [RFC 7748]**.

Application Note: The TOE generates ECDH private and public value that are used in SSH and TLS key exchange.

The TLS uses all the curves (P-256, P-384, P-521 and X25519, X448), while the SSH only uses X25519.

6.2.2.3 FCS_CKM.1/ED25519 Cryptographic key generation

FCS_CKM.1.1/ED25519 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ED25519** and specified cryptographic key size of **256 bits** that meet the following: **[RFC 8032].**

Application Note: The TOE uses the ED25519 keygen method to generate the 'SSH host key' which is used as the client key within the SFTP protocol. For ED25519 key generation the DRG.3 random number generator of the TOE will be used.

6.2.2.4 FCS_CKM.2/DH Cryptographic key establishment

FCS_CKM.2.1/DH The TSF shall ~~distribute~~perform cryptographic key~~s~~ establishment in accordance with a specified cryptographic key ~~distribution~~establishment method: **Finite field-based key establishment schemes** that meet the following: **[NIST SP800-56A**]**.**

Application Note: When establish TLS communications, the TOE generates a shared secret value with the peer during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption, and generation and verification of integrity protection information for TLS communication. The key generation is performed according to [RFC5246] [RFC6347] and [RFC8446].

6.2.2.5 FCS_CKM.2/ECDH Cryptographic key establishment

FCS_CKM.2.1/ECDH The TSF shall perform cryptographic key establishment in accordance with specified cryptographic key establishment methods: **Elliptic curve-based key establishment schemes** using NIST curves P-256, P-384, P-521; and X25519 and X448, that meet the following: **[NIST SP800-56A]**.

Application Note: When establishing SSH/TLS communications, the TOE generates a shared secret value with the peer during the ECDH key agreement. The shared secret value is used to derive session keys used for encryption and decryption, and generation and verification of

Copyright © Huawei Technologies Co., Ltd.

integrity protection information for SSH/TLS communication. The key generation is performed according to [RFC 4253], [RFC5246], [RFC8446] and [RFC6347].

6.2.2.6 FCS_CKM.4/Volatile Cryptographic key destruction

FCS_CKM.4.1/volatile The TSF shall destroy cryptographic keys in volatile memory in accordance with a specified cryptographic key destruction method **deallocation of the resource** that meets the following: **none.**

Application Note: Whenever a Trusted Channel is terminated for whatever reason, all temporary keying material (e.g. DH/ECDH values) and session keys are erased from the volatile memory by the post-processing routines associated with the Trusted Channel.

6.2.2.7 FCS_CKM.4/ED25519 Cryptographic key destruction

FCS_CKM.4.1/ED25519 The TSF shall destroy cryptographic ED25519 keys in accordance with a specified cryptographic key destruction method **by overwriting with 0** that meets the following: **none**

Application Note: This SFR was refined to ED25519 keys in the non-volatile memory only. The ED25519 keys will be stored in flash memory of the SCC board. The private key cannot be exported. Whenever an SSH session is terminated for whatever reason, the destruction operation of ED25519 keys can be executed by the Administrator.

6.2.2.8 FCS_COP.1/AES Cryptographic operation

FCS_COP.1.1/AES The TSF shall perform **symmetric decryption and encryption** in accordance with a specified cryptographic algorithm **AES with operating modes as specified in Table 6-1** and cryptographic key sizes **as specified in Table 6-1** that meet the following: **standards as specified in Table 6-1.**

Table 6-1 AES operating modes supported by the TOE for symmetric decryption and encryption

AES operating mode	**Cryptographic key sizes [bits]**	**Meeting the standards**
GCM mode	128, 256	[FIPS 197], [NIST SP800-38D]
CTR mode	128, 192, 256	[FIPS 197], [NIST SP800-38A]
CCM mode	128	[FIPS 197], [NIST SP800-38C]

Application Note: AES-128, 192, 256 in CTR mode is used for encryption and decryption within SSH communication.

AES-128/256 in GCM mode is used for encryption and decryption within TLS/DTLS communication.

AES-128 in CCM mode is used for encryption and decryption within TLS communication.

6.2.2.9 FCS_COP.1/CHACHA Cryptographic operation

FCS_COP.1.1/CHACHA The TSF shall perform **symmetric decryption and encryption** in accordance with a specified cryptographic algorithm **CHACHA20-POLY1305** and cryptographic key sizes **256 bits** that meet the following: **[RFC 8439]**.

Copyright © Huawei Technologies Co., Ltd.

Application Note: CHACHA20-POLY1305 is used for encryption and decryption within TLS v1.3 and DTLS v1.2 communication.

6.2.2.10 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1/RSA The TSF shall perform **signature generation and verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **3072 bits to 4096 bits** that meet the following: **[FIPS 186-4], Section 5,5, using PKCS#1 V1.5 Signature Scheme RSASSA-PKCS#1-v1.5 and PKCS#1 V2.1 Signature Scheme RSASSA-PSS.**

Application Note: The TOE supports the generation of RSA key pairs in PKCS #1 v1.5 format with key lengths of 3072 bits. For TLS certificate signature verification, both PKCS #1 v1.5 (RSASSA-PKCS1-v1.5) and PKCS #2.1 (RSASSA-PSS) are supported, with key lengths ranging from 3072 to 4096 bits. (TLS cipher suites refer to Section 8.2.1)

RSA key and certificate used by TLS are provided by the operational environment, see A.TLSKeyandCertificate.

6.2.2.11 FCS_COP.1/ED25519 Cryptographic operation

FCS_COP.1.1/ED25519 The TSF shall perform **signature generation and verification** in accordance with a specified cryptographic algorithm **ED25519** and cryptographic key sizes **256 bits** that meet the following: **[RFC 8032].**

Application Note: ED25519 with key size of 256 bits according to [RFC 8032] is used for "publickey" authentication of the TOE (as SFTP client) to the server for SSH according to chap. 7 [RFC 4252].

6.2.2.12 FCS_COP.1/HMAC-SHA256 Cryptographic operation

FCS_COP.1.1/HMAC-SHA256 The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA256** and cryptographic key sizes **256 bits** that meet the following: [**RFC 2104], [FIPS 180-4].**

Application Note: HMAC-SHA256 is used in the TLS and SSH communications according to [RFC 5246], [RFC 8446], [RFC 6347] and [RFC 6668]. HMAC-SHA256 is used in NTP authentication according to [RFC 8573].

6.2.2.13 FCS_COP.1/HMAC-SHA384 Cryptographic operation

FCS_COP.1.1/HMAC-SHA384 The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA384** and cryptographic key sizes **384 bits** that meet the following: [**RFC 2104], [FIPS 180-4].**

Application Note: HMAC-SHA384 is used in the TLS communication according to [RFC [RFC 5246], [RFC 8446] and [RFC 6347].

6.2.2.14 FCS_COP.1/HMAC-SHA512 Cryptographic operation

FCS_COP.1.1/HMAC-SHA512 The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA512** and cryptographic key sizes **512 bits** that meet the following: [**RFC 2104], [FIPS 180-4].**

Application Note: HMAC-SHA512 is used in the SSH communication according to [RFC 6668].

Copyright © Huawei Technologies Co., Ltd.

6.2.2.15 FCS_COP.1/SHA256 Cryptographic operation

FCS_COP.1.1/SHA256 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA256** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA256 is used in TLS and SSH communications.

6.2.2.16 FCS_COP.1/SHA384 Cryptographic operation

FCS_COP.1.1/SHA384 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA384** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA384 is used in TLS communication.

6.2.2.17 FCS_COP.1/SHA512 Cryptographic operation

FCS_COP.1.1/SHA512 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA512** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA512 is used in SSH and TLS communication.

6.2.2.18 FCS_COP.1/PBKDF2 Cryptographic operation

FCS_COP.1.1/PBKDF2 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **PBKDF2(HMAC-SHA256) with iteration number 10000** and cryptographic key sizes **None** that meet the following: **[RFC 8018].**

Application Note: PBKDF2 is used for hashing passwords before storage in non-volatile memory. The salt used in PBKDF2 is a 16 byte size random number obtained from the TOE's deterministic random number generator.

6.2.2.19 FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1 The TSF shall provide a ***deterministic*** random number generator that implements:

- **DRG.3.1: If initialized with a random seed of 32 bytes that shall contain at least 128 bit entropy the internal state of the RNG shall have Min-entropy of at least 100 bits.**
- **DRG.3.2: The DRNG provides forward secrecy.**
- **DRG.3.3: The DRNG provides backward secrecy even if the current internal state is known.**

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

- **DRG.3.4: The RNG, initialized with a random seed of 256 bits during the preparative operations ensured by the preparative procedures for users generates output for which more than 2^{14} strings of bit length 128 are mutually different with probability greater than $1-2^{-8}$.**
- **DRG.3.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A and no other test suites.**

Copyright © Huawei Technologies Co., Ltd.

Application Note: The operations have been performed according to chap. 4.8 of [AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 128 bits entropy. The seed value is provided by the hardware TPM chip integrated in the SCC. The TOE will seed the DRNG at the module initialization stage before start of TLS-based communication and SSH-based communication.

The DRNG complies with [NIST SP 800-90A] using HMAC-DRBG (SHA-256).

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **user group SFP** on

Subject: users;

Objects: commands provided by TOE;

Operation: Execute

6.2.3.2 FDP_ACF.1 Security Attribute based Access Control

FDP_ACF.1.1 The TSF shall enforce the **user group SFP** to objects based on the following:

Subject security attributes

users and their following security attributes:

- **username**
- **user group**

Objects security attributes:

commands and their following security attributes:

- **Command level (There are five command levels: Monitor, Operate, Maintain, Manage, Debug)**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. **Only authorized users are permitted execute commands.**
2. **Users can be configured with different user group to execute command with different command levels.**
3. **There are four user groups: Monitor, Operator, Maintainer, Administrator, in ascending order of privilege level.**
4. **Each user group corresponds to different command levels. A user can execute all commands from the command level corresponding to his user group and below.**

Table 6-2 Correspondence of user groups and command levels

User group	Command Level
Monitor	Monitor
Operator	Monitor Operate

Copyright © Huawei Technologies Co., Ltd.

Maintenance	Monitor Operate Maintenance
Administrator	Monitor Operate Maintenance Manage Debug

5. **The command level is stored by the TOE and cannot be changed.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

6.2.3.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the **Management Network Traffic Flow Filtering SFP** on

Subjects:

Device management interface

Information:

IP packets

Operations:

Device management interface will accept or deny IP packets based on the settings of the device management interface and the IP packets content (i.e. subject attributes and information security attributes as defined in chap. 6.2.3.4).

6.2.3.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **Management Network Traffic Flow Filtering SFP** based on the following types of subject and information security attributes

Subject: Device management interface

Subject attributes:

- **IP address (i.e. IP address setting of the device management interface)**
- **Port number**

Information: IP packets

Information security attributes:

- **Source IP address**

Copyright © Huawei Technologies Co., Ltd.

- **Source wildcard**
- **Destination IP address**
- **Destination wildcard**
- **Protocol type**
- **Source port**
- **Destination port**
- **ICMP protocol type**
- **ICMP code type**

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

1. **Whenever an incoming IP packet to the device management interface is handled by TCP/IP protocol layer 3 (forwarding or accepting) on TOE, the Access Control List (ACL) will be checked.**
2. **The ACL rules could either permit or deny accepting based on the Subject attributes of the device management interface, as well as Information security attributes. Rules have to contain at least one of the attributes but may contain several attributes.**
3. **For every incoming IP packet to the device management interface that is intended to be accepted by the TOE the ACL is checked for a rule that matches the attributes of the packet, respectively starting from the first entry in the ACL. The ACL is checked until the first matching rule is found. The IP packet is then either accepted or discarded according to the matching rule in the ACL. If no matching rule is found, the packet is accepted.**

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

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

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **none.**

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when ***an administrator configurable positive integer within* 1 to 10** unsuccessful authentication attempts occur related to **user logging in**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met*,** the TSF shall

1. lock the offending username;

2. audit the event in the security log.

Application Note: The default value for the maximum number of consecutive failed logins is five, and the interval between two attempts is shorter than three minutes.

Copyright © Huawei Technologies Co., Ltd.

6.2.4.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. username

2. user validity period

3. user group

4. password

5. password validity period

6. the inactivity time after which an account is automatically logged out.

7. status of the account (locked/unlocked)

8. number of failed consecutive logins within certain period of time and timestamp of last successful login

9. identity of the terminal that a user logs in from.

6.2.4.3 FIA_UAU.2 User authentication before any action

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

Application Note: Authentication is possible by username and password.

6.2.4.4 FIA_UAU.5 Multiple Authentication Mechanisms

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

1. Remote authentication by RADIUS for authentication;

2. Local Authentication by local database of the TOE for authentication

to support user authentication.

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

1. For Remote authentication by RADIUS;

2. For local Authentication, the TSF will authenticate the users based on the configured Identification (including username and password).

Application Note: Users can access the TOE through the RMT or LMT. Both the RMT and LMT support local authentication and RADIUS authentication. The TOE can use only one of the mechanisms at any given time. The Administrator can configure which mechanism is used by the TOE.

6.2.4.5 FIA_UID.2 User identification before any action

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

Application Note: Authentication is possible by username and password. The user is identified by his username if he is able to successfully authenticate with his username and corresponding password.

Copyright © Huawei Technologies Co., Ltd.

6.2.4.6 FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **Username**
- **User Group**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **None**.

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

Application Note: The TOE subjects of relevance are management sessions.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine the behavior of*** the functions **defined in FMT_SMF.1** to **users with sufficient user group as defined in FMT_SMR.1**.

6.2.5.2 FMT_MSA.1/ACFATD Management of Security Attributes (user group SFP)

FMT_MSA.1.1/ACFATD The TSF shall enforce the **user group SFP** to restrict the ability to ***query, modify*** the security attributes **identified in FDP_ACF.1 and FIA_ATD.1** to **the users with sufficient user group as defined in FMT_SMR.1**.

6.2.5.3 FMT_MSA.1/IFF Management of Security Attributes

FMT_MSA.1.1/IFF The TSF shall enforce the **Management Network Traffic Flow Filtering SFP** to restrict the ability to ***delete, modify*** the security attributes **identified in FDP_IFF.1** to **users with sufficient user group as defined in FMT_SMR.1**

6.2.5.4 FMT_MSA.3/ACFATD Static Attribute Initialization

FMT_MSA.3.1/ACFATD The TSF shall enforce the **user group SFP** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ACFATD The TSF shall allow **users with sufficient user group as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 FMT_MSA.3/IFF Static Attribute Initialization

FMT_MSA.3.1/IFF The TSF shall enforce the **Management Network Traffic Flow Filtering SFP** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/IFF The TSF shall allow **users with sufficient user group as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

Copyright © Huawei Technologies Co., Ltd.

6.2.5.6 FMT_SMF.1 Specification of Management Functions

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

1. **Management of user accounts and user attributes, including user credentials**
2. **Management of authentication failure policy**
3. **Management of ACLs and ACL parameters like IP addresses or address ranges**
4. **Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP**
5. **Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces**
6. **Management of the TOE's time**

6.2.5.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. **Monitor (as defined in the table below)**
2. **Operator (as defined in the table below)**
3. **Maintenance (as defined in the table below)**
4. **Administrator (as defined in the table below)**

Role	Authority
Monitor	This group has the lowest authority. The accounts of this group are authorized to issue query commands and modify some of their own attributes.
Operator	The accounts of this group are authorized to query the system information and perform some configuration operations.
Maintenance	The accounts of this group are authorized to perform all maintenance operations, including the authority of Operator group and general maintenance and diagnosis operations
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations. Especially, Administrators are also authorized to perform the advanced diagnosis (debug) operation.

Application Note: The roles are hierarchical, i.e. each role includes all authorities of the previous roles in addition to the authorities described for the role itself.

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

Copyright © Huawei Technologies Co., Ltd.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable Timestamps

FPT_STM.1.1 The TSF shall be able to provide reliable timestamps.

6.2.7 TOE access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **a time interval of user inactivity which can be configured.**

6.2.7.2 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

1. authentication failure

2. Source IP address

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_ITC.1/TLS Inter-TSF trusted channel

FTP_ITC.1.1/TLS The TSF shall provide a communication channel between itself and another trusted IT product 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.

Application Note: To establish a trusted channel, the TLS protocol shall be used. TLS complies with RFC 5246 (TLS1.2), and RFC 8446 (TLS1.3), DTLS compiles with RFC 6347(DTLS1.2).

FTP_ITC.1.2/TLS The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

Application Note: The TSF will act as TLS client to initiate communication to the Syslog server which acts as TLS server.

FTP_ITC.1.3/TLS The TSF shall initiate communication via the trusted channel for **transmission of audit data to Syslog server**.

6.2.8.2 FTP_ITC.1/SFTP Inter-TSF trusted channel

FTP_ITC.1.1/SFTP The TSF shall provide a communication channel between itself and another trusted IT product 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.

FTP_ITC.1.2/SFTP The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

FTP_ITC.1.3/SFTP The TSF shall initiate communication via the trusted channel for **file transfer via SFTP**.

Application Note: To establish a trusted channel, the SSH(SFTP) protocol shall be used. SFTP complies with [RFC 4251], [RFC 4252], [RFC 4253], and [RFC 4254].

Copyright © Huawei Technologies Co., Ltd.

For SSH/SFTP-based communications the following algorithms and ciphers are supported:

- Authentication can be performed either public key-based or password-based as described in [RFC 4252].

  The SFTP authentication policy is determined by the SFTP server. As an SFTP client, the TOE supports the two authentication modes.

  And, The TOE will authenticate the SFTP server using public-key. You need to obtain the public key fingerprint of an SFTP server through an official channel and configure it on the TOE.

- Key exchange is performed using curve25519-sha256 provides strong (~128 bits) security.
- The public key algorithm of the SSH transport implementation is ED25519.
- For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported.
- For data integrity protection HMAC_SHA2_256 and HMAC_SHA2_512 are supported.

6.2.8.3 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***remote, local*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***modification, disclosure***.

Application Note: To establish a trusted path from LMT/RMT to the TSF, the TLS protocol shall be used. TLS complies with RFC 5246 (TLS1.2), and RFC 8446 (TLS1.3).

Client authentication is performed password-based on the application layer.

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

Application Note: The LMT/RMT will act as TLS client to initiate communication to the TOE which acts as TLS server.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***management of the TOE***.

Application Note: The TSF offers the ability for protected communication for user sessions.

6.3 Security Functional Requirements Rationale

6.3.1 Coverage

As shown Table 6-3 provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Copyright © Huawei Technologies Co., Ltd.

Table 6-3 Mapping SFRs to objectives

Security Functional Requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_STG.1	O.Audit
FAU_STG.3	O.Audit
FCS_COP.1/AES FCS_COP.1/CHACHA FCS_COP.1/RSA FCS_COP.1/ED25519 FCS_COP.1/HMAC-SHA256 FCS_COP.1/HMAC-SHA384 FCS_COP.1/HMAC-SHA512 FCS_COP.1/SHA256 FCS_COP.1/SHA384 FCS_COP.1/SHA512	O.Communication
FCS_COP.1/PBKDF2	O.Authentication, O.PasswordHash
FCS_CKM.1/DH FCS_CKM.1/ECDH FCS_CKM.1/ED25519	O.Communication
FCS_CKM.2/DH FCS_CKM.2/ECDH	O.Communication
FCS_CKM.4/Volatile FCS_CKM.4/ED25519	O.Communication
FCS_RNG.1	O.Communication
FDP_ACC.1	O.Authorization
FDP_ACF.1	O.Authorization
FDP_IFC.1	O.DataFilter
FDP_IFF.1	O.DataFilter
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_UAU.2	O.Authentication

Copyright © Huawei Technologies Co., Ltd.

FIA_UAU.5	O.Authentication
FIA_UID.2	O.Authentication O.Authorization
FIA_USB.1	O.Audit O.Authentication O.Authorization
FMT_MOF.1	O.Authorization O.SecurityManagement
FMT_MSA.1/ACFATD	O.Authorization O.SecurityManagement
FMT_MSA.1/IFF	O.Authorization O.DataFilter O.SecurityManagement
FMT_MSA.3/ACFATD	O.Authorization O.SecurityManagement
FMT_MSA.3/IFF	O.Authorization O.DataFilter O.SecurityManagement
FMT_SMF.1	O.Authorization O.SecurityManagement O.DataFilter
FMT_SMR.1	O.Authorization O.SecurityManagement
FPT_STM.1	O.Audit
FTA_SSL.3	O.Authentication O.Communication
FTA_TSE.1	O.DataFilter O.Authentication O.Communication
FTP_ITC.1/TLS	O.Communication O.Authentication O.Audit
FTP_ITC.1/SFTP	O.Authentication O.Communication
FTP_TRP.1	O.Authentication O.Communication

Copyright © Huawei Technologies Co., Ltd.

6.3.2 Sufficiency

As shown Table 6-4 provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Copyright © Huawei Technologies Co., Ltd.

Table 6-4 SFR sufficiency analysis

Copyright © Huawei Technologies Co., Ltd.

Security objective	Rationale
O.DataFilter	The requirement of ACL is defined in FDP_IFF.1 and FDP_IFC.1 and the impact on session establishment is covered in FTA_TSE.1. The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/IFF, FMT_MSA.3/IFF and FMT_SMF.1. Rejection of connections is addressed by FTA_TSE.1.
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by FPT_STM.1 and user identities as defined in FAU_GEN.2 where applicable. User identities are available through binding management sessions to their users (FIA_USB.1). Requirements on reading audit records are defined in FAU_SAR.1 and FAU_SAR.2. The protection of the stored audit records against unauthorized modification is implemented in FAU_STG.1. If the audit trail exceeds the size of the storage device The TSF shall roll back the oldest records as required by FAU_STG.3. Secure transmission of audit data to external Syslog server is enforced by FTP_ITC.1/TLS

Copyright © Huawei Technologies Co., Ltd.

O.Communication	Communication security is implemented by the establishment of trusted paths for users in FTP_TRP.1 and trusted channels towards the Syslog server and SFTP server in FTP_ITC.1/TLS and FTP_ITC.1/SFTP. Termination of inactive sessions is covered by FTA_SSL.3. FTA_TSE.1 addresses that session establishment is denied if an ACL exists that specifies a deny rule for the attempted connection. FCS_COP.1/AES, FCS_COP.1/CHACHA, FCS_COP.1/RSA, FCS_COP.1/ED25519, FCS_COP.1/HMAC-SHA256, FCS_COP.1/HMAC-SHA384, FCS_COP.1/HMAC-SHA512, FCS_COP.1/SHA256, FCS_COP.1/SHA384 and FCS_COP.1/SHA512 are providing the cryptographic functions required for TLS and SFTP channels. Password-based user authentication requires password hashing provided by FCS_COP.1/PBKDF2. FCS_CKM.1/ED25519 addresses key generation of ED25519 keys. FCS_CKM.1/DH and FCS_CKM.1/ECDH address generation of DH and ECDH private and public values, respectively. FCS_CKM.2/DH and FCS_CKM.2/ECDH address establishment of session keys for TLS and SSH. FCS_CKM.4/Volatile addresses destruction of keying material and session keys in volatile memory. FCS_CKM.4/ED25519 addresses destruction of ED25519 key in non-volatile memory. Note that keys of AES and HMAC algorithms as a result of the DH/ECDH key agreement are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are overwritten upon session termination according to FCS_CKM.4/Volatile. The allocated memory is freed as well. Random numbers needed for secure communication are addressed by FCS_RNG.1.
O.Authentication	User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. Remote user authentication by RADIUS as well as authentication via local database is implemented by FIA_UAU.5. The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1 and the subjects acting on the behalf of that user are addressed in FIA_USB.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1. For password verification hash values of passwords are used which are generated using FCS_COP.1/PBKDF2. User authentication via RMTs/LMTs requires the use of a trusted path according to FTP_TRP.1 and a trusted channel according to FTP_ITC.1/TLS and FTP_ITC.1/SFTP. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1.

Copyright © Huawei Technologies Co., Ltd.

O.Authorization	User identification is addressed in FIA_UID.2. Usernames and user groups are bound to management sessions and available for access control decisions through user-subject binding (FIA_USB.1). The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. User-related attributes are spelled out in FIA_ATD.1 and the subjects acting on the behalf of that user are spelled out in FIA_USB.1 Security Management is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1, FMT_SMF.1 and FMT_MOF.1. Requirements on the management functionality for the definition of access control policies and other security functions behavior, security attributes, and static attribute initialization are provided in FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ ACFATD, and FMT_MSA.3/IFF.
O.Security Management	The requirements on management of security functions behavior, security attributes, and static attribute initialization are provided in FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD, FMT_MSA.3/IFF, and FMT_SMF.1. The management functionality for the security functions of the TOE is defined in FMT_SMF.1 and the security user roles are defined in FMT_SMR.1.
O.PasswordHash	Password hashing is implemented by FCS_COP.1/PBKDF2.

6.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again. The augmentation by ALC_FLR.2 does not cause any additional dependencies.

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.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Table 6-5 Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1

Copyright © Huawei Technologies Co., Ltd.

Security Functional Requirement	Dependency	Resolution
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported [FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], fulfilled by FCS_CKM.2/DH and FCS_CKM.2/ECDH instead. FCS_CKM.4/Volatile
FCS_COP.1/CHACHA	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported [FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], fulfilled by FCS_CKM.2/ECDH instead. FCS_CKM.4/Volatile
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]; FCS_CKM.4
FCS_COP.1/ED25519	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/ED25519 FCS_CKM.4/ED25519
FCS_COP.1/HMAC-SHA512	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported [FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], fulfilled by FCS_CKM.2/DH and FCS_CKM.2/ECDH instead. FCS_CKM.4/Volatile
FCS_COP.1/HMAC-SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported [FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], fulfilled by FCS_CKM.2/DH and FCS_CKM.2/ECDH instead. FCS_CKM.4/Volatile
FCS_COP.1/HMAC-SHA384	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported [FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], fulfilled by FCS_CKM.2/DH and FCS_CKM.2/ECDH instead. FCS_CKM.4/Volatile

Copyright © Huawei Technologies Co., Ltd.

Security Functional Requirement	Dependency	Resolution
FCS_COP.1/SHA512	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4
FCS_COP.1/SHA384	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4
FCS_CKM.1/DH	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_CKM.2/DH FCS_CKM.4/Volatile
FCS_CKM.1/ECDH	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_CKM.2/ECDH FCS_CKM.4/Volatile
FCS_CKM.1/ED25519	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/ED25519 FCS_CKM.4/ED25519
FCS_CKM.2/DH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/Volatile
FCS_CKM.2/ECDH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/ECDH FCS_CKM.4/Volatile
FCS_CKM.4/Volatile	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/DH and FCS_CKM.1/ECDH
FCS_CKM.4/ED25519	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/ED25519
FCS_RNG.1	No Dependencies	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1

Copyright © Huawei Technologies Co., Ltd.

Security Functional Requirement	Dependency	Resolution
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3/ACFATD
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3/IFF
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	No Dependencies	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	No Dependencies	None
FIA_UID.2	No Dependencies	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/ACFATD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/IFF	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/ACFATD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ACFATD FMT_SMR.1
FMT_MSA.3/IFF	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/IFF FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	No Dependencies	None
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_ITC.1/TLS	No Dependencies	None
FTP_ITC.1/SFTP	No Dependencies	None
FTP_TRP.1	No Dependencies	None

Copyright © Huawei Technologies Co., Ltd.

6.3.4 Justification for unsupported dependencies

The following dependencies are unsupported for the reasons given below.

FCS_COP.1/AES, FCS_COP.1/CHACHA: session keys are established using DH/ECDH key establishment method, so FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 are not supported. Instead FCS_CKM.2/DH and FCS_CKM.2/ECDH are used to fulfill the dependencies.

FCS_COP.1/SHA256, FCS_COP.1/SHA384, FCS_COP.1/SHA512, FCS_COP.1/PBKDF2: Hash functions do not require keys, so FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, and FCS_CKM.4 are not applicable.

FCS_COP.1/HMAC-SHA256, FCS_COP.1/HMAC-SHA384 and FCS_COP.1/HMAC-SHA512: session keys are established using DH/ECDH key establishment method, so FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 are not supported. Instead FCS_CKM.2/DH and FCS_CKM.2/ECDH are used to fulfill the dependencies.

FCS_COP.1/RSA: The RSA key and certificate used for TLS are imported(see A.TLSKeyandCertificate), so FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.4 are not applicable.

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the EAL3 augmented with ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

6.5 Security Assurance Requirements Rationale

The EAL3 augmented with ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL package selected (EAL3) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here. The augmentation by ALC_FLR.2 does not cause any additional dependencies.

Copyright © Huawei Technologies Co., Ltd.

7 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

7.1 Authentication

The TOE can identify users based on unique IDs and enforce their authentication before granting them access to any TSF management interfaces in Table 7-1. Detailed functions include:

- Support authentication via local username and password. The user password length ranges from 8 to 128 characters. By default, the minimum password length is set to 12 characters. This function is achieved by comparing user information input with pre-defined user information stored in the flash. The pre-defined user information (reference data) is the user password hashed using the PBKDF2 function as defined in the 'Cryptographic Functions' TOE Security Function.
- Support authentication via the remote RADIUS authentication server. The TOE hands username and password provided by the user during login to the RADIUS server and enforces the RADIUS server’s pass/fail decision.
- Support logout when no operation is performed on the user session within a specified interval. If an account that has logged in does not exchange information with the TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login. By default, the inactivity period is 10 minutes. The inactivity period ranges from 5 to 60 minutes
- Support maximum attempts for authentication failures within certain period of time. The default value of maximum attempts is 5, the configurable range is between 1 and 10. After maximum login attempts using one account fail and the interval between two attempts is shorter than 3 minutes, the account is locked. An alarm is reported after the account is locked. The default value of lock period is 15 minutes, the configurable range is between 1 and 1000 minutes. So the user account will be automatically unlocked after 15 minutes by default.
- Support access limit by IP-based ACL.
- The TOE stores the following security attributes for individual users: username, user validity period, user group, password, password validity period, the inactivity time after which an account is automatically logged out, status of the account (locked/unlocked), number of failed consecutive logins within certain period of time and timestamp of last successful login, and identity of the terminal that a user logs in from.

Copyright © Huawei Technologies Co., Ltd.

- Using the SFTP application requires Administrator users to unlock the private ED25519 key for SFTP first with the key's passphrase. When the key is generated, the Administrator is allowed to set a passphrase of 12 to 16 characters.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FIA_USB.1, FCS_COP.1/PBKDF2, FTA_TSE.1, FTA_SSL.3, FTP_TRP.1)

Table 7-1 SFR to TSF mapping

SFR	TSF
FIA_AFL.1	Support maximum attempts for authentication failures within certain period of time. The default value of maximum attempts is 5, the configurable range is between 1 and 10. After maximum login attempts using one account fail and the interval between two attempts is shorter than 3 minutes, the account is locked. An alarm is reported after the account is locked.
FIA_ATD.1 FIA_USB.1	Support authentication via local username and password. Passwords have a length of 8 to 128 characters. This function is achieved by comparing user information input with pre-defined user information stored in the flash. Using the SFTP application requires Administrator users to unlock the private ED25519 key for SFTP first with the key's passphrase. When the key is generated, the Administrator must set a passphrase of 12 to 16 characters. The TOE stores the following security attributes for individual users: username, user validity period, user group, password, password validity period, the inactivity time after which an account is automatically logged out, status of the account (locked/unlocked), number of failed consecutive logins within certain period of time and timestamp of last successful login, and identity of the terminal that a user logs in from.
FIA_UAU.2	The TOE enforces that every user needs to successfully authenticate himself by username and password before he can use any TOE security function other than the identification and authentication function.
FIA_UAU.5	Support authentication via local username and password. This function is achieved by comparing user information input with pre-defined user information stored in the flash. Support authentication via the remote RADIUS authentication server. The TOE hands username and password information provided by the user during login to the RADIUS server and enforces the RADIUS server's pass/fail decision.
FIA_UID.2	The TOE enforces that every user is successfully identified by username when providing username and password for authentication before he can use any TOE security function other than the identification and authentication function.

Copyright © Huawei Technologies Co., Ltd.

FCS_COP.1/PBKDF2	The pre-defined user information (reference data) is the user password hashed using the PBKDF2 (HMAC-SHA256) function as defined in the 'Cryptographic Functions' TOE Security Function.
FTA_TSE.1	Support access limit by IP-based ACL.
FTA_SSL.3	Support logout when no operation is performed on the user session within a specified interval. If an account that has logged in does not exchange information with the TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login. By default, the inactivity period is 10 minutes. The inactivity period ranges from 5 to 60 minutes
FTP_TRP.1	The TOE provides communication security by implementing trusted paths between the RMT/LMT and the TOE using the TLS communication protocol. The TLS1.2 and TLS1.3 protocols are supported.

7.2 Authorization

The TOE enforces an access control by supporting following functions in Table 7-2:

- There are four hierarchical user groups (from low to high): Monitor, Operator, Maintenance, and Administrator.
- A user group is assigned to each account.
- Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed and the attempt is audited. The authority of each user group is specified in Table 7-2.
- Every management command has a *command level* associated to it. A user can use this command if his user group dominates the command level, i.e., if his user group is hierarchically equal or higher than the command level. User groups match to command levels as follows:

Table 7-2 Correspondence of user groups and command levels

User group	Command Level
Monitor	Monitor
Operator	Monitor Operate
Maintenance	Monitor Operate Maintenance
Administrator	Monitor Operate

Copyright © Huawei Technologies Co., Ltd.

	Maintenance Manage Debug

- In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user group and cannot increase the user group attribute beyond their own user group. Command levels cannot be changed by users.
- Only Administrators can query and dump operation logs and security logs.

(FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UID.2, FIA_USB.1, FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.3/ACFATD, FMT_SMF.1, FMT_SMR.1)

Table 7-3 SFR to TSF mapping

SFR	TSF
FDP_ACC.1	Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed and the attempt is audited. The authority of each user group is specified in Table 7-2. In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user group and cannot increase the user group attribute beyond their own user group. Command levels cannot be changed by users.
FDP_ACF.1, FIA_ATD.1, FIA_UID.2, FIA_USB.1	There are four hierarchical user groups (from low to high): Monitor, Operator, Maintenance and Administrator. A user group is assigned to each account. Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed and the attempt is audited. The authority of each user group is specified in Table 7-2. Every management command has a command level associated to it. A user can use this command if his user group dominates the command level, i.e., if his user group is hierarchically equal or higher than the command level. Only Administrators can query and dump operation logs and security logs. The TOE enforces that every user is successfully identified by username when providing username and password for authentication before he can use any TOE security function other than the identification and authentication function.
FMT_MOF.1	Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an

Copyright © Huawei Technologies Co., Ltd.

	error message is displayed and the attempt is audited. The authority of each user group is specified in Table 7-2. Every management command has a command level associated to it. A user can use this command if his user group dominates the command level, i.e., if his user group is hierarchically equal or higher than the command level. Only Administrators can query and dump operation logs and security logs.
FMT_MSA.1/ACFATD FMT_MSA.3/ACFATD FMT_SMF.1	Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed and the attempt is audited. The authority of each user group is specified in Table 7-2. Every management command has a command level associated to it. A user can use this command if his user group dominates the command level, i.e., if his user group is hierarchically equal or higher than the command level. Only Administrators can query and dump operation logs and security logs.
FMT_SMR.1	There are four hierarchical user groups (from low to high): Monitor, Operator, Maintenance and Administrator. A user group is assigned to each account. Only Administrators can query and dump operation logs and security logs.

7.3 Auditing

The TOE provides an audit trail consisting of operation logs and security logs:

- Support recording non-query operations in the operation logs, including the operation type (if applicable), operation object (if applicable), access IP address (if applicable), date and time, the outcome, and username (if applicable).
- Support recording security-related configuration operations in the security logs, including user management, security settings, and the attempts of unauthorized operations. The security logs provide the information about the account name, address of the client, date and time, operation, and outcome.
- For all audit events the corresponding timestamp will be recorded together with the event.
- Only Administrators can query and dump operation logs and security logs, and the Administrators can know that whoever accesses and logins the system and any operation on the system according to the content of the security log and the operation log.
- The operation logs and security logs allow no manual changes.
- The operation logs and security logs can be completely recovered even after a power-outage restart of the system.
- The operation logs and security logs keep records in time sequence. After the memory is exhausted, the earliest records of the logs are overwritten by the latest records. Once the memory is exhausted, a performance event is reported.

Copyright © Huawei Technologies Co., Ltd.

- Support for user individual attributes including the username ensures that each user is unique in the system and that user-related audit events can be attributed to a user.
- All logs contain a reliable time stamp.
- The TOE initiate communication via the trusted channel for transmission of audit data to Syslog server.

(FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3, FIA_USB.1, FPT_STM.1, FTP_ITC.1/TLS)

Table 7-4 SFR to TSF mapping

SFR	TSF
FAU_GEN.1	Support recording non-query operations in the operation logs, including the operation type, operation object, access IP address, date and time, the outcome, and username. Support recording security-related configuration operations in the security logs, including user management, security settings, and the attempts of unauthorized operations. The security logs provide the information about the account name, address of the client, date and time, operation, and outcome. For all audit events the corresponding timestamp will be recorded together with the event.
FAU_GEN.2	Support recording non-query operations in the operation logs, including the operation type, operation object, access IP address, date and time, the outcome, and username.
FAU_SAR.1 FAU_SAR.2	Only Administrators can query and dump operation logs and security logs. So only the Administrators can know that whoever accesses and logins the system and any operation on the system according to the content of the security log and the operation log.
FAU_STG.1	The operation logs and security logs allow no manual changes.
FAU_STG.3	The operation logs and security logs can be completely recovered even after a power-outage restart of the system. The operation logs and security logs keep records in time sequence. After the memory is exhausted, the earliest records of the logs are overwritten by the latest records. Once the memory is exhausted, a performance event is reported.
FIA_USB.1	Support for user individual attributes including the username ensures that each user is unique in the system and that user-related audit events can be attributed to a user.
FPT_STM.1	All logs contain a reliable time stamp.
FTP_ITC.1/TLS	The TOE initiate communication via the trusted channel for transmission of audit data to Syslog server

Copyright © Huawei Technologies Co., Ltd.

7.4 Communication Security

The TOE provides communication security by implementing trusted paths/channels between the RMT/LMT and the TOE and between the TOE and the Syslog server using the TLS communication protocol. The TLS1.2 and TLS1.3 protocols are implemented to provide communication channels. The TOE acts as a TLS server when communicating with RMT/LMT and allows them to initiate communication. The TOE acts as a TLS client when communicating with the Syslog server and initiates communication. The TLS certificates for server/client authentication are managed and issued by users. For RMT/LMT client authentication is performed password-based on the application layer. The TOE has been loaded with a preset TLS certificate before delivery.

The following TLS ciphers are supported by the TOE:

TLS1.2:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

TLS1.3:

- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC8446
- TLS_AES_256_GCM_SHA384 as defined in RFC8446
- TLS_AES_128_GCM_SHA256 as defined in RFC8446
- TLS_AES_128_CCM_SHA256 as defined in RFC8446

The communication protocol between RMT and TOE is QX over TLS or MML over TLS, while the communication protocol between LMT and TOE is QX over TLS:

- QX is a proprietary machine-machine interface, and it is used for GUI interfaces. RMT/LMT uses graphical interface to provide various management and maintenance functions, and the communication protocol is QX. TOE provides abundant QX commands to allow the users to manage the TOE.
- The MML interface is a proprietary man-machine interface with character string format, and it is a CLI interface. Like QX, MML is an application layer protocol protected by TLS, but MML commands is delivered through the command line terminal. MML commands can be sent through the "Transport Command Tool", which is integrated in NCE(RMT).

The TOE provides secure communication based on the DTLS protocol and provides a secure communication channel between the TOE and the RADIUS server to ensure communication security. The TOE supports DTLS1.2.

In DTLS-based secure communication, the TOE words as a DTLS client and initiates communication with the RADIUS server. DTLS certificates used for server authentication are managed and issued by users. The TOE supports DTLS certificate loading and activation. The pre-configured DTLS certificate has been loaded to the TOE before delivery.

Huawei preset certificates used by TLS and DTLS by default. And the TOE supports import user-defined certificates.

Copyright © Huawei Technologies Co., Ltd.

The following DTLS ciphers are supported by the TOE:

- ECDHE_RSA_CHACHA20_POLY1305 as defined in RFC 8439
- ECDHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5289
- ECDHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5289
- DHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5288
- DHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5288

The TOE provides communication security by establishing a trusted channel for secure file transfer based on the SSH(SFTP) protocol. The TOE acts as a SFTP client which initiates communication with other trusted IT products. The SSH/SFTP-based communication is based on the following algorithms and ciphers, for details of the cipher, please refer to chapter 7.8:

- Authentication can be performed either public key-based or password-based as described in RFC 4252.
- Key exchange is performed using curve25519-sha256 provides strong (~128 bits) security.
- The public key algorithm of the SSH transport implementation is ED25519.
- For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported.
- For data integrity protection HMAC-SHA256 and HMAC-SHA512 are supported.

The TOE supports session time-out after a configurable time of user inactivity. After the session has expired, the equipment user account will be automatically logged out.

The TOE supports denying session establishment based on authentication failure (i.e. device authentication failure for TLS and user authentication as well as device authentication failure for SFTP).

The TOE supports denying session establishment based on source IP address with is based on the ACL mechanisms of the Management Traffic Flow Control TOE Security Function.

(FTA_SSL.3, FTA_TSE.1, FTP_ITC.1/TLS, FTP_ITC.1/SFTP, FTP_TRP.1)

Table 7-5 SFR to TSF mapping

SFR	TSF
FTA_SSL.3	The TOE supports session time-out after a configurable time of user inactivity. After the session has expired, the equipment user account will be automatically logged out.
FTA_TSE.1	The TOE supports denying session establishment based on authentication failure (i.e. device authentication failure for TLS and user authentication as well as device authentication failure for SFTP). The TOE supports denying session establishment based on source IP address with is based on the ACL mechanisms of the Management Traffic Flow Control TOE Security Function.
FTP_ITC.1/TLS	The TOE provides communication security by implementing trusted channels between the Syslog server and the TOE using

Copyright © Huawei Technologies Co., Ltd.

	the TLS communication protocol. The TLS1.2 and TLS1.3 protocol are implemented to provide communication channels. The TOE acts as a TLS client and initiates communication. The TLS certificates for client authentication are managed and issued by users. The TOE supports TLS certificate loading and activation. The TOE has been loaded with a preset TLS certificate before delivery. The following TLS ciphers are supported by the TOE: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 TLS_CHACHA20_POLY1305_SHA256 as defined in RFC8446 TLS_AES_256_GCM_SHA384 as defined in RFC8446 TLS_AES_128_GCM_SHA256 as defined in RFC8446 TLS_AES_128_CCM_SHA256 as defined in RFC8446 The TOE provides secure communication based on the DTLS protocol and provides a secure communication channel between the TOE and the RADIUS server to ensure communication security. The TOE supports DTLS1.2. In DTLS-based secure communication, the TOE words as a DTLS client and initiates communication with the RADIUS server. DTLS certificates used for server authentication are managed and issued by users. The TOE supports DTLS certificate loading and activation. The pre-configured DTLS certificate has been loaded to the TOE before delivery. The following DTLS ciphers are supported by the TOE: ECDHE_RSA_CHACHA20_POLY1305 as defined in RFC 8439 ECDHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5289 ECDHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5289 DHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5288 DHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5288
FTP_ITC.1/SFTP	The TOE provides communication security by establishing a trusted channel for secure file transfer based on the SSH(SFTP) protocol. The TOE acts as a SFTP client which initiates communication with other trusted IT products. The SSH/SFTP-based communication is based on the following algorithms and ciphers: Authentication can be performed either public key-based or password-based as described in RFC 4252. Key exchange is performed using curve25519-sha256 provides strong (~128 bits) security.The public key algorithm of the SSH transport implementation is ED25519.

Copyright © Huawei Technologies Co., Ltd.

	For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported. For data integrity protection HMAC-SHA256 and HAMC-SHA512 are supported.
FTP_TRP.1	The TOE provides communication security by implementing trusted paths between the RMT/LMT and the TOE using the TLS communication protocol. The TLS1.2 and TLS1.3 protocol are supported. The TOE acts as a TLS server and allows the RMT/LMT to initiate communication. The TLS certificates for server authentication are managed and issued by users. The TOE supports TLS certificate loading and activation. Client authentication is performed password-based on the application layer. The TOE has been loaded with a preset TLS certificate before delivery. For the supported TLS ciphers please see FTP_ITC.1/TLS above.

7.5 Traffic Flow Control

The TOE uses ACL to deny unwanted network traffic on management interfaces and allow wanted network traffic on management interfaces.

The "management interfaces" is "ETH interfaces", "ETH interfaces" are dedicated to the TOE management, and all devices (RMT/LMT/SFTP/RADIUS/SYSLOG/NTP) are connected to the TOE through ETH interfaces. All traffic passing through the ETH interfaces is filtered.

IP-based ACL is provided to filter traffic flow on management interfaces by matching all or some attributes, including the source IP address, source wildcard, destination IP address, destination wildcard, IP protocol type, TCP/UDP source port, TCP/UDP destination port, ICMP protocol type and ICMP code type, and then performs actions such as permit, or discard accordingly.

(FDP_IFC.1, FDP_IFF.1, FMT_MSA.1/IFF, FMT_MSA.3/IFF, FMT_SMF.1, FTA_TSE.1)

Table 7-6 SFR to TSF mapping

SFR	TSF
FDP_IFC.1	The TOE uses ACL to deny unwanted network traffic on management interfaces and allow wanted network traffic on management interfaces.
FDP_IFF.1, FMT_MSA.1/IFF, FMT_MSA.3/IFF	IP-based ACL is provided to filter traffic flow on management interface by matching all or some attributes, including the source IP address, source wildcard, destination IP address, destination wildcard, IP protocol type, TCP/UDP source port, TCP/UDP destination port, ICMP protocol type and ICMP code type, and then performs actions such as permit, or discard accordingly. The TOE enforces application of ACLs to IP packets from the management network. By default, no ACL rules are configured therefore all traffic will be allowed to pass. Users with sufficient user group can add, delete and modify ACL rules. The ACL

Copyright © Huawei Technologies Co., Ltd.

	rules will take effect immediately after they are added. The ACL filtering mechanism does only accept connections that are explicitly permitted in the ACL filtering rules. By adding corresponding ACL rules, users with sufficient user group can change the default behavior where all traffic is allowed to pass.
FMT_SMF.1	The TOE supports creation, modification and deletion of ACLs.
FTA_TSE.1	The TOE supports denying session establishment based on source IP address with is based on the ACL mechanisms of the Management Traffic Flow Control TOE Security Function.

7.6 Security Management

The TOE offers management functionality for its security functions. Security management functionality can either be used through LMT or RMT. And TLS must be used.

The access control mechanisms of the TOE are based on hierarchical access levels where a user group is associated with every user on the one hand and a command level is associated with every command. Only if the user group is equal or higher to a specific command, the user is authorized to execute this command. Management of security function is realized through QX or MML commands. So, for every management function sufficient user group is required for the user to be able to execute the corresponding command.

Modifications have to be saved; otherwise they will be lost after reboot of the TOE. The TOE loads the saved device configuration during start-up, so saved modifications are not lost by rebooting the device. After reset to factory defaults, the TOE is in the factory configuration.

The security management functionality comprises:

- The TOE support configuration of ACLs based on the source IP address, source wildcard, destination IP address, destination wildcard, IP protocol type, TCP/UDP source port, TCP/UDP destination port, ICMP protocol type and ICMP code type;
- Support configuration on limiting access for remote administration by IP address;
- The TOE supports the configuration of the minimum time a user account is blocked after failed attempts for user authentication;
- The TOE supports the management of user accounts (creating, maintaining, and deleting user accounts) and user data (username, password including password reset). The TOE supports the assignment of user groups to users;
- The TOE supports the configuration of the output host and output channel for audit data (e.g. output to external audit servers);
- The TOE supports SFTP for secure file transfer.
- The TOE supports the configuration of the authentication policy including local authentication and remote authentication via RADIUS.
- The TOE supports the configuration of local time and time synchronization policy via NTP, and the Administrator have the privilege to configure or modify the NTP configuration.

(FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD, FMT_MSA.3/IFF, FMT_SMF.1, FMT_SMR.1)

Copyright © Huawei Technologies Co., Ltd.

Table 7-7 SFR to TSF mapping

SFR	TSF
FMT_MOF.1 FMT_MSA.3/ACFATD FMT_SMR.1	The access control mechanisms of the TOE are based on hierarchical access levels where a user group is associated with every user on the one hand and a command level is associated with every command. Only if the user group is equal or higher to a specific command, the user is authorized to execute this command. Management of security function is realized through QX or MML commands. So, for every management function sufficient user group is required for the user to be able to execute the corresponding command.
FMT_MSA.1/ACFATD	The TOE supports the management of user accounts (creating, maintaining, and deleting user accounts) and user data (username, password including password reset). The TOE supports the assignment of user groups to users; for every management function sufficient user group is required for the user to be able to execute the corresponding command.
FMT_MSA.1/IFF FMT_MSA.3/IFF	The TOE support configuration of ACLs based on the source IP address, source wildcard, destination IP address, destination wildcard, IP protocol type, TCP/UDP source port, TCP/UDP destination port, ICMP protocol type and ICMP code type; By default, no ACL rules are configured therefore all traffic will be allowed to pass. Users with sufficient user group can add, delete and modify ACL rules. The ACL rules will take effect immediately after they are added. The ACL filtering mechanism does only accept connections that are explicitly permitted in the ACL filtering rules. By adding corresponding ACL rules, users with sufficient user group can change the default behavior where all traffic is allowed to pass.
FMT_SMF.1	The TOE supports the following management functions: 1. Management of user accounts and user attributes, including user credentials 2. Management of authentication failure policy 3. Management of ACLs and ACL parameters like IP addresses or address ranges 4. Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP 5. Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces 6. Management of the TOE's time

Copyright © Huawei Technologies Co., Ltd.

7.7 Cryptographic functions

Cryptographic functions are required by security features as dependencies. The following cryptographic algorithms are supported:

1) The TOE supports symmetric encryption and decryption using the AES algorithm. The TOE support the following algorithms.

   GCM mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP800-38D]**

   GCM mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP800-38D]**

   CTR mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP800-38A]**

   CTR mode, and cryptographic key sizes **192bits** that meet the following: [**FIPS 197], [NIST SP800-38A]**

   CTR mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP800-38A]**

   CCM mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP800-38C]**

   AES-128/192/256 in CTR mode is used for encryption and decryption within SSH communication.

   AES-128/256 in GCM mode is used for encryption and decryption within TLS/DTLS communication.

   AES-128 in CCM mode is used for encryption and decryption within TLS communication.

2) The TOE supports symmetric encryption and decryption using the CHACHA20-POLY1305 algorithm for TLS 1.3 and DTLS 1.2 communication.

3) The TOE supports signature generation and verification using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PSS with a key length of 3072 or 4096 bits for TLS.

4) The TOE supports keyed-hash message authentication using the HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512 algorithm according to [FIPS 180-4]. HMAC-SHA256 and HMAC-SHA512 are used for the SSH communication. HMAC-SHA256 and HMAC-SHA384 are used for the TLS communication. For all cipher suites defined in [RFC 5246] and [RFC 3268] it is used especially for data integrity protection. (For TLS cipher suites that use GCM or CCM mode, the mechanism is used only for TLS PRF/HKDF.)

5) The TOE supports SHA-256, SHA-384 and SHA-512 hashing function. SHA-256 and SHA-512 are used for the SSH communication. SHA-256, SHA-384 and SHA-512 are used for the TLS communication.

6) The TOE supports hashing of data using PBKDF2 (HMAC-SHA256) algorithm according to [RFC 8018] for password hashing. The iteration number is 10000. The salt used in PBKDF2 is a 16 byte size random number obtained from the TOE's deterministic random number generator.

7) The TOE supports establishment of cryptographic keys using Diffie-Hellman key exchange and specified cryptographic key sizes 3072 and 4096 bits according to [NIST SP800-56A] for TLS.

8) The TOE supports establishment of cryptographic keys using Elliptic Curve Diffie-Hellman key exchange with NIST curves P-256, P-384, P-521, X25519, X448 according to [NIST SP800-56A] for TLS, only X25519(CURVE25519) for SSH.

Copyright © Huawei Technologies Co., Ltd.

9) The TOE supports key generation for the ED25519 algorithm according to [RFC 8032]. The generated keys have a key length of 256 bits and are intended for usage in SSH.
10) The TOE supports destruction of temporary keying material (e.g. DH/ECDH values) and session keys used for secure communication channels based on TLS or SFTP which are stored in volatile memory by erasing the corresponding area in memory reserved for the corresponding session. So the keying material and session keys are destroyed by the post-processing routines of the underlying trusted channel which are executed whenever a session is terminated for any reason.
11) The TOE supports the destruction of ED25519 keys by overwriting with '0'.
12) The TOE supports the SSH protocol according to [RFC 4251], [RFC 4252], [RFC 4253], [RFC 4254] and the following cipher suites]:
    - curve25519-sha256 as key exchange algorithm of SSH.
    - AES-128-CTR/ AES-192-CTR/ AES-256-CTR encryption and decryption algorithm.
    - ED25519 according to [RFC 8709] for "publickey" authentication of the TOE (client) to the server.
    - HMAC-SHA256 and HMAC-SHA512 data integrity generation and verification algorithm.
13) The operations have been performed according to chap. 4.8 of [AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 128 bit entropy. The seed value is provided by the hardware TPM chip integrated in the SCC. The system check the status of TPM chip with minutes level. If the check fails, logs and alarms are generated for alert, notice the Administrator to perform active/standby switchover, and replace the faulty SCC board.
    The DRNG complies with [NIST SP800-90A] using HMAC-DRBG (SHA-256).

    (FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_CKM.2/DH, FCS_CKM.2/ECDH, FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA256, FCS_COP.1/HMAC-SHA384, FCS_COP.1/HMAC-SHA512, FCS_COP.1/SHA256, FCS_COP.1/SHA384, FCS_COP.1/SHA512, FCS_COP.1/PBKDF2, FCS_CKM.4/Volatile, FCS_CKM.4/ED25519, FCS_RNG.1, FCS_COP.1/CHACHA)

Table 7-8 SFR to TSF mapping

SFR	TSF
FCS_COP.1/AES	The TOE supports symmetric encryption and decryption using the AES algorithm. The TOE supports the following algorithms. GCM mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP800-38D]** GCM mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP800-38D]** CTR mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP800-38A]** CTR mode, and cryptographic key sizes **192bits** that meet the following: [**FIPS 197], [NIST SP800-38A]** CTR mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP800-38A]** CCM mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP800-38C]** AES-128/192/256 in CTR mode is used for encryption and decryption within SSH communication. AES-128/256 in GCM mode is used for encryption and

Copyright © Huawei Technologies Co., Ltd.

	decryption within TLS communication. AES-128 in CCM mode is used for encryption and decryption within TLS communication.
FCS_COP.1/CHACHA	The TOE supports symmetric encryption and decryption using the CHACHA20-POLY1305 algorithm for TLS 1.3 and DTLS 1.2 communication.
FCS_COP.1/RSA	The TOE supports signature generation and verification using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PSS with a key length of 3072 or 4096 bits for TLS.
FCS_COP.1/ED25519	The TOE supports signature generation and verification using the ED25519 algorithm according to [RFC 8032] with a key length of 256 bits for SSH.
FCS_COP.1/HMAC-SHA256 FCS_COP.1/HMAC-SHA384 FCS_COP.1/HMAC-SHA512	The TOE supports keyed-hash message authentication using the HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512 algorithm according to [FIPS 180-4]. This mechanism is used for the SSH/TLS communication. For all cipher suites defined in [RFC 5246] and [RFC 3268] it is used especially for data integrity protection. (For TLS cipher suites that use GCM or CCM mode, the mechanism is used only for TLS PRF/HKDF.)
FCS_CKM.1/DH FCS_CKM.2/DH	The TOE supports establishment of cryptographic keys using Diffie-Hellman key exchange with key sizes 3072 and 4096 bits according to [NIST SP800-56A] for TLS.
FCS_CKM.1/ECDH FCS_CKM.2/ECDH	The TOE supports establishment of cryptographic keys using Elliptic Curve Diffie-Hellman key exchange with NIST curves P-256, P-384 and P-521 according to [FIPS 186-4] and X25519 and X448 according to [RFC 7748] for TLS, only X25519(CURVE25519) for SSH.
FCS_COP.1/SHA256 FCS_COP.1/SHA384 FCS_COP.1/SHA512	SHA256, SHA384 and SHA512 are used in SSH/TLS communication as hashing function.
FCS_COP.1/PBKDF2	The TOE supports hashing of data using PBKDF2 (HMAC-SHA256) algorithm according to [RFC 8018] for password hashing. The iteration number is 10000. The salt used in PBKDF2 is a 16 byte size random number obtained from the TOE's deterministic random number generator.
FCS_CKM.4/Volatile	The TOE supports destruction of temporary keying material (e.g. DH/ECDH values) and session keys used for secure communication channels based on TLS or SFTP which are stored in volatile memory by erasing the corresponding area in memory reserved for the corresponding session. So the keying material and session keys are destroyed by the post-processing routines of the underlying trusted channel which are executed whenever a session is terminated for any reason.
FCS_CKM.4/ED25519	The TOE supports the destruction of ED25519 keys by overwriting with '0'.
FCS_RNG.1	The operations have been performed according to chap. 4.8 of

Copyright © Huawei Technologies Co., Ltd.

	[AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 128 bit entropy. The seed value is provided by the hardware TPM chip integrated in the SCC. The TOE ensures that TLS-based communication and SSH-based communication cannot be enabled before the DRNG is seeded. The DRNG complies with [NIST SP800-90A] using HMAC-DRBG (SHA-256).

Copyright © Huawei Technologies Co., Ltd.

8 Crypto Disclaimer

8.1 SSH

8.1.1 Cryptographic statement

Only SSHv2 (SFTP client) is supported in the evaluated configuration.

Table 8-1 Cryptographic functionality of SSH implemented

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Comments
1	Authentication	ED25519	[RFC 8709]	256 bits	Pubkeys are exchanged trustworthily out of band, e.g. checking fingerprints. Authenticity is not part of the TOE. (no certificates are used)
2		Username and password-based authentication	[RFC 4252], sec. 8 (SSH-AUTH) for user authentication Method: “password”	Guess success prob.	The client authenticates either with Username & password or by cryptographic means as shown in #1. Password-based authentication is set by default. The security level depends on the server policy.
3	Key agreement (key exchange)	curve25519-sha256	[RFC 8731]	256 bits	
4	Confidentiality	AES in CTR mode (aes128-ctr, aes192-ctr, aes256-ctr)	[FIPS 197] (AES), [NIST SP800-38A] (CTR) [RFC 4344] [RFC 4253] (SSH-	|k|=128, 192, 256	Binary packet protocol: encryption

Copyright © Huawei Technologies Co., Ltd.

			TRANS)		
5	Integrity and authenticity	HMAC SHA2 256 、HMAC_SHA2_512	[RFC 2104], [FIPS 198-1] (HMAC) [RFC 4251] / [RFC 4253] (SSH HMAC support) [RFC 6668]	|k|=256,512	Message authentication
6	Key generation	ED25519 key generation	[RFC 8032] section 5.1.5	N/A	Generation of Host keys and user keys acc. to FCS_CKM.1/ED25519 Using FCS_RNG.1
7	Trusted channel	FTP_ITC.1/SFTP [ST], sec. 6.2.8.2	See above	N/A	The security level depends on the server policy.

8.2 Transport Security Layer protocol

Only TLS 1.2, TLS 1.3 and DTLS 1.2 are supported in the evaluated configuration.

8.2.1 Cryptographic statement

Table 8-2 Cryptographic functionality of TLS implemented

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size [Bits]	Comments
1	Authentication (server)	X.509 certificates	[RFC 5246] (TLS1.2), [RFC 8446](TLS 1.3), [RFC 6347](DTLS 1.2)	N/A	
2		RSA signature verification and generation RSASSA-PSS using SHA-256 RSASSA-PSS using SHA-384 RSASSA-PSS using SHA-512 RSASSA-PKCS1-v1.5 using SHA-256 RSASSA-PKCS1-v1.5 using SHA-384 RSASSA-PKCS1-v1.5 using SHA-512	[RFC 3447] (PKCS#1 v2.1) [RFC 2313] (PKCS#1 v1.5) [RFC 5246] (TLSv1.2), [RFC 6347] (DTLSv1.2), [FIPS 186-4], B.3 [FIPS 180-4] (SECURE HASH ALGORITHMS) [RFC 8446]	Modulus length: 3072 to 4096 bits	Certificates with Key Usage
3	Authentication (client)	X.509 certificates	[RFC 5246] (TLS1.2), [RFC 8446](TLS 1.3), [RFC 6347](DTLS 1.2)	N/A	

Copyright © Huawei Technologies Co., Ltd.

4		RSA signature verification and generation RSASSA-PSS using SHA-256 RSASSA-PSS using SHA-384 RSASSA-PSS using SHA-512 RSASSA-PKCS1-v1.5 using SHA-256 RSASSA-PKCS1-v1.5 using SHA-384 RSASSA-PKCS1-v1.5 using SHA-512	[RFC 3447] (PKCS#1 v2.1) [RFC 2313] (PKCS#1 v1.5) [RFC 5246] (TLSv1.2), [RFC 6347](DTLS 1.2), [FIPS 186-4], B.3 [FIPS 180-4] (SECURE HASH ALGORITHMS) [RFC 8446]	Modulus length: 3072 to 4096 bits	Certificates with Key Usage
5	Key agreement (key exchange)	Diffie–Hellman: Elliptic Curve Diffie-Hellman	[RFC 3526] (for the group diffie-hellman-group 15,diffie-hellman-group 16) [RFC 5246](TLS 1.2) [RFC 8446](TLS 1.3) [RFC 6347](DTLS 1.2) [NIST SP800-56A](DH) [PKCS#3]	|k|=3072, 4096	
6	Key derivation	PRF: HMAC with SHA-256, SHA-384 (default: prf sha256 for TLSv1.2, also prf_sha384 possible)	[RFC 2104] (HMAC) [FIPS 180-4] (SECURE HASH ALGORITHMS) [RFC 5246](TLSv1.2) [RFC 6347](DTLS 1.2)	N/A	
7	Confidentiality	AES-128 in GCM mode AES-256 in GCM mode AES-128 in CCM mode CHACHA20	[FIPS 197] (AES) [NIST SP800-38D] (GCM) [RFC 5288] (AES GCM within TLS) [RFC8446] [RFC8439]	|k|=128, 256	
8	Integrity	HMAC with SHA-256 or SHA-384	[FIPS 180-4] (SECURE HASH ALGORITHMS)	|k|= 256 ,384	Message authentication code (record layer)
9	Trusted channel	FTP_ITC.1/TLS [ST], sec. 6.2.8.1 FTP_TRP.1 [ST],sec. 6.2.8.3	Cf. all lines above	N/A	

Copyright © Huawei Technologies Co., Ltd.

8.2.2 Supported TLS cipher suites

The supported TLS cipher suites in the evaluated configuration are:

- tls1.2 CipherSuite：
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- tls1.3 CipherSuite：
- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC8446
- TLS_AES_256_GCM_SHA384 as defined in RFC8446
- TLS_AES_128_GCM_SHA256 as defined in RFC8446
- TLS_AES_128_CCM_SHA256 as defined in RFC8446
- dtls1.2 CipherSuite:
- ECDHE_RSA_CHACHA20_POLY1305 as defined in RFC 8439
- ECDHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5289
- ECDHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5289
- DHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5288
- DHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5288

8.3 Password hashing

8.3.1 Cryptographic statement

User login password hashing & local sensitive data encryption.

Table 8-3 Cryptographic functionality of password hashing implemented

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size [Bits]	Comments
1	Authentication	PBKDF2 (HMAC-SHA256,10000 iterations)	[RFC 8018]	N/A	Hashing for password storage Iteration number is 10000

Copyright © Huawei Technologies Co., Ltd.

A Abbreviations, Terminology and References

A.1 Abbreviations

ADSL	Asymmetric Digital Subscriber Line
APIU	AC Power Interface Unit
ASON	Automatically Switched Optical Network
BRAS	Broadband Remote Access Server
CC	Common Criteria
CTU	system control and communication board with clock processing function
CXP	cross connect, system control and clock processing board
DCI	Data Center Interconnect
DCN	Data Communications Network (the management network)
EFI	External Functionality Interface
ETH	Ethernet
HCXP	Hybrid cross connect, system control and clock processing board
LMT	Local Maintenance Terminal
MON32	optical backplane insertion loss detection and tunable-bandwidth optical power detection board
ODUk	Optical Channel Data Unit - k
OSN	Optical Switch Node
OTN	Optical Transport Network
PIU	Power Interface Unit
PP	Protection Profile
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial-In User Service
RMT	Remote Maintenance Terminal
RSA	Rivest Shamir Adleman

Copyright © Huawei Technologies Co., Ltd.

SDH	Synchronous Digital Hierarchy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
VC	Virtual Channel
WDM	Wavelength Division Multiplexing
UCXCS	Universal Cluster CROSS-Connect and Synchronous timing board

A.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.

Administrator: An Administrator in the content is the user of Administrator group

User: A user is a human or a product/application using the TOE.

A.3 References

[AIS20] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017

[FIPS 180-4] FIPS PUB 180-4 – Secure Hash Standard (SHS)

[FIPS 186-4] FIPS PUB 186-4 – Digital Signature Standard (DSS), July 2013

[FIPS 197] FIPS PUB 197 – Advanced Encryption Standard (AES), November 26, 2001

[FIPS 198-1] FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC), July 2008

[NIST SP800-38A] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001

[NIST SP800-38C] NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, May 2004

Copyright © Huawei Technologies Co., Ltd.

[NIST SP800-38D]	NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007
[NIST SP800-56A]	NIST Special Publication 800-56A Rev. 3 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018
[NIST SP800-90A]	NIST Special Publication 800-90A Rev. 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
[PKCS#1 V2.1]	PKCS #1 v2.1: RSA Cryptography Standard, April 2004
[PKCS#3]	PKCS #3: Diffie-Hellman Key- Agreement Standard, version 1.4, November 1993
[RFC 2104]	RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997
[RFC 3268]	*Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*, P. Chown, June 2002
[RFC 3447]	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications, Version 2.1, J. Jonsson, B. Kaliski, 2003-02-01
[RFC 3526]	RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003
[RFC 4251]	RFC 4251 – The Secure Shell (SSH) Protocol Architecture, January 2006
[RFC 4252]	RFC 4252 - The Secure Shell (SSH) Authentication Protocol, January 2006
[RFC 4253]	RFC 4253 - The Secure Shell (SSH) Transport Layer Protocol, January 2006
[RFC 4254]	RFC 4254 - The Secure Shell (SSH) Connection Protocol, January 2006
[RFC 4344]	The Secure Shell (SSH) Transport Layer Encryption Modes, M. Bellare, T. Kohno, C. Namprempre, 2006-01-01
[RFC 5246]	RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, August 2008
[RFC 5288]	AES Galois Counter Mode (GCM) Cipher suited for TLS, J. Salowey, A. Choudhury, D. McGrew 2008-08-01
[RFC 6347]	Datagram Transport Layer Security Version 1.2
[RFC 6668]	The scrypt Password-Based Key Derivation Function
[RFC 7748]	Elliptic Curves for Security, January 2016
[RFC 8018]	PKCS #5: Password-Based Cryptography Specification Verion 2.1, B. Kaliski, 2017-01-01
[RFC 8032]	Edwards-Curve Digital Signature Algorithm (EdDSA), January 2017
[RFC 8439]	ChaCha20 and Poly1305 for IETF Protocols, June 2018
[RFC 8446]	The Transport Layer Security (TLS) Protocol Version 1.3, August 2018

Copyright © Huawei Technologies Co., Ltd.

[RFC 8709] Ed25519 and Ed448 Public Key Algorithms for the Secure Shell (SSH) Protocol, February 2020

[RFC 8731] Secure Shell (SSH) Key Exchange Method Using Curve25519 and Curve448, February 2020

Copyright © Huawei Technologies Co., Ltd.