Huawei OptiX OSN9800 series product CSPN

Security Target

Issue 4.0

Date 2023-05-04

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

About This Document

Change History

Date	Revision Version	Change description	Author
2022-12-07	Ver 3.0	This is the initial draft for CSPN application.	Diao Runan
2023-05-05	Ver 4.0	Corrected some misleading descriptions.	Diao Runan, Wang Baogang

Contents

Figures & Tables

1 Introduction

1.1 Product identification

This Security Target is the Huawei OptiX OSN 9800 software component.

Manufacturer	Huawei Technologies Co., Ltd
Organization URL	https://www.huawei.com/en/
Product's commercial name	Huawei OptiX OSN 9800 software component
Product software's version	V100R022C10
Patch version	SPC100
Reference model	Reference model for OSN9800: OptiX OSN 9800 M12
Additional models for the range	Additional models for OSN9800: OptiX OSN 9800 M24, OptiX OSN 9800 M05
Guidance document	OSN 9800 V100R022C10 Product Documentation

1.2 Abbreviations

SDH	Synchronous Digital Hierarchy
WDM	Wavelength Division Multiplexing
OTN	Optical Transmission Network
LAN	Local Area Network
OSN	Optical Switching Network
SCC	System Control and Communication
TDM	Time Division Multiplexing
EMS	Element Management System
LUN	Logic Unit Number
UTS	Unified Transmission Software
IPC	Inter Process communication
RMT	Remote Management Terminal
SSH	Secure Shell

SFTP	Secure File Transfer Protocol
FTP	File Transfer Protocol
NTP	Network Time Protocol
DNS	Domain Name System
ACL	Access Control List
TOE	Target of Evaluation
TSF	TOE Security Function
TLS	Transport Layer Security

2 Product and TOE description

2.1 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 2-1, 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.

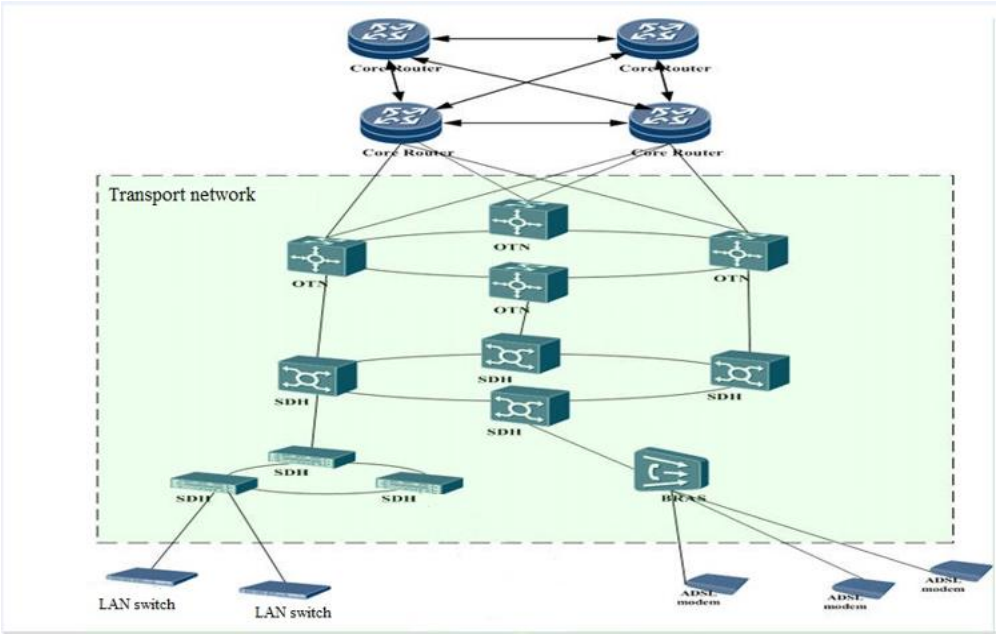


Figure 2-1 position of the transmission network on the entire communication network

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:

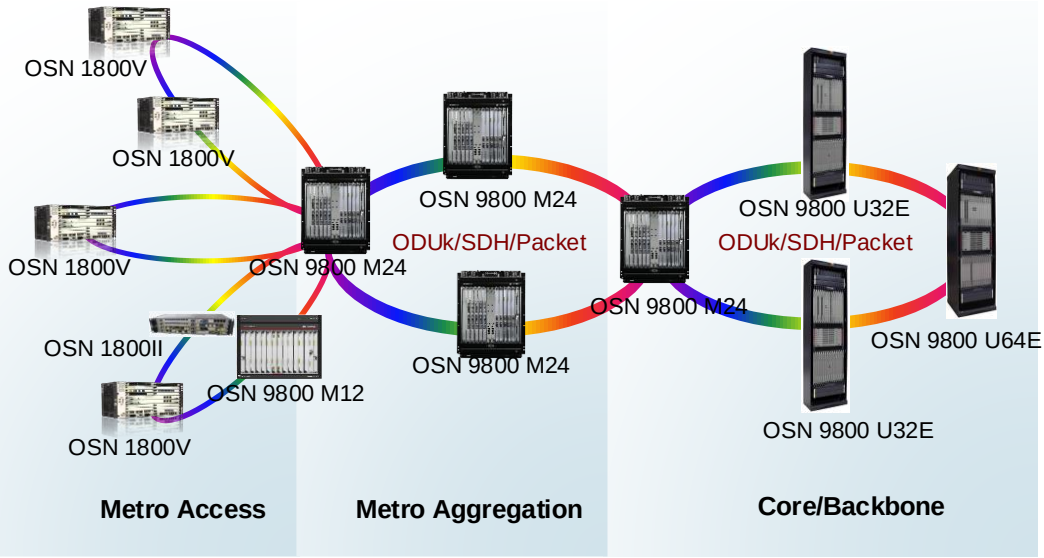
- The access layer of the network,
- The metro or aggregation layer of the network,
- The core or backbone core layer of the network.

The access layer of the network is mainly responsible for the access control of the services of individual and enterprise users. The metro or aggregation layer of the network is to converge the massive user traffic and connect the access layer and backbone or core layer of network. The role of the backbone or core layer of the network is to provide the export of the network, connect with

all backbone 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 M24/M12/M05 devices are mainly applicable to the metro or aggregation layer of the metropolitan area network and the core or backbone layer of the Backbone networks as shown in Figure below. Services such as OTN, Packet, and SDH services are processed at the access layer and then sent to the convergence node / backbone / core on the metro transmission network. In this manner, the OptiX OSN 9800 M24/M12/M05 works with the current OptiX WDM equipment to extend the services to the access layer.

Position of the OptiX OSN 9800 M24/M12/M05 on the entire network



2.2 Hardware Architecture

This section will introduce OptiX OSN 9800 M24/M12/M05 from a physical architectural point of view and a software architectural point of view.

The OptiX OSN 9800 M24/M12/M05 is transmission equipment and is mainly applicable to the core/backbone and metro/aggregation layer of the transmission network. Services such as OTN, Packet, and SDH services are processed at the metro access layer and then sent to the convergence node on the metro transmission network.

The OptiX OSN 9800 M24/M12/M05 devices consists of the hardware and the software.

As shown in Figure 2-2 to **Error! Reference source not found.**Figure 2-4 System architecture of the OptiX OSN 9800 M05, 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, consisting of OTN line board, Optical layer board, Packet board, and TDM board etc.

Figure 2-2 System architecture of the OptiX OSN 9800 M24

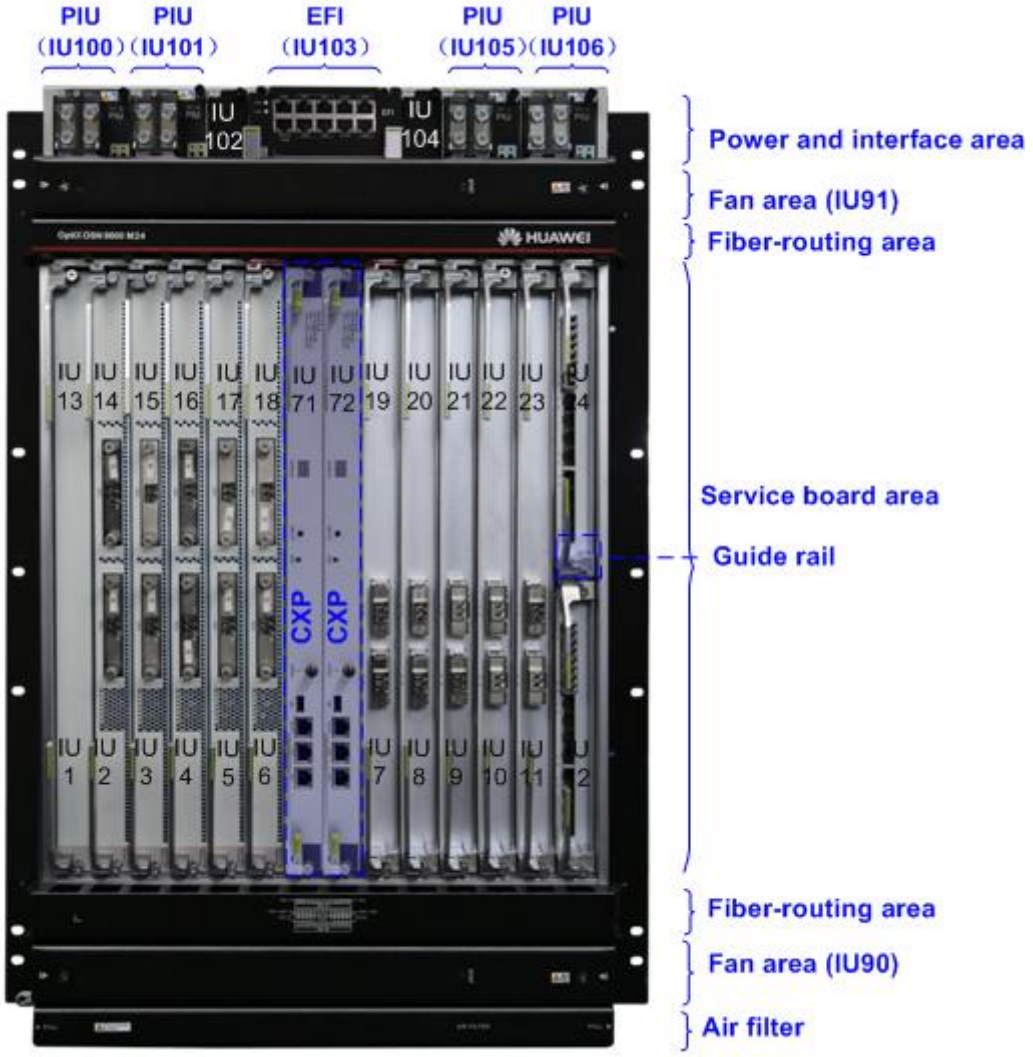


Figure 2-3 System architecture of the OptiX OSN 9800 M12

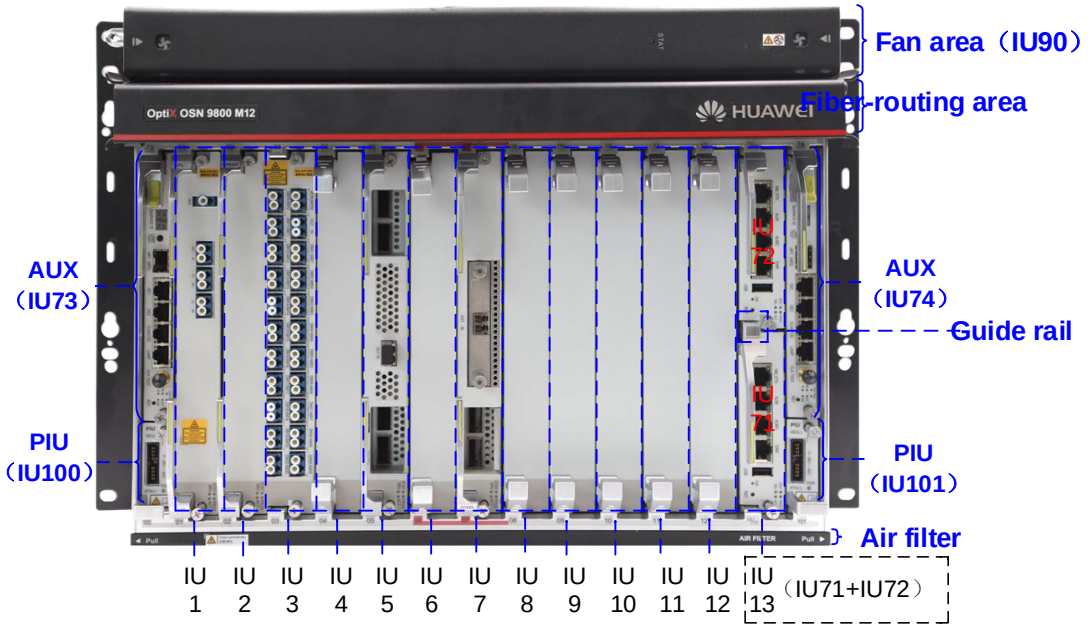
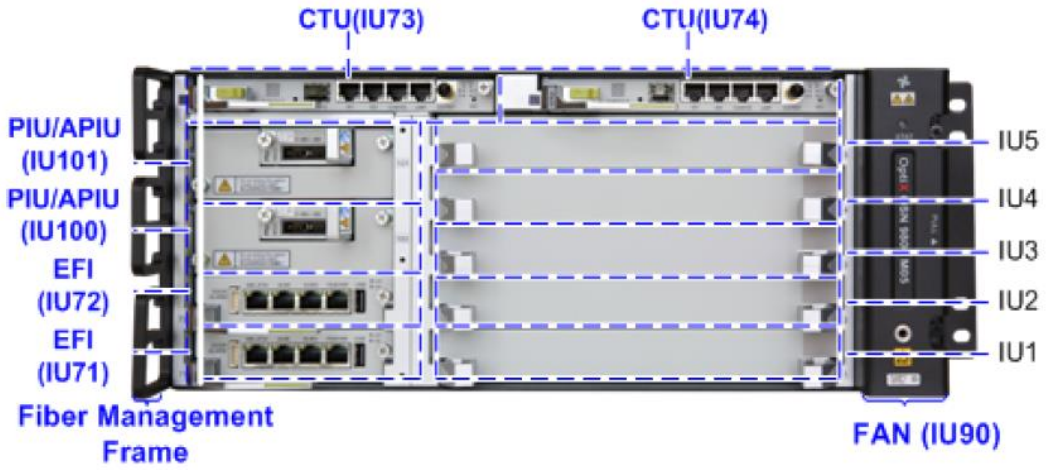


Figure 2-4 System architecture of the OptiX OSN 9800 M05



The service units are responsible for signal amplifying, optical transpondering, optical multiplexing and demultiplexing, optical add and drop multiplexing etc., in which a board software is running.

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. Every chassis have two SCC boards and they work in 1+1 backup mode.

The OptiX OSN 9800 M24/M12/M05 software is deployed in the SCC unit and service units. The part of the OptiX OSN 9800 M24/M12/M05 software deployed in the SCC unit includes UTS and other service application components. UTS is a platform software, which is responsible for managing and controlling the all software units, and is responsible for communication with external management network entities including EMS or SSH client, RADIUS server, SFTP server and syslog server etc., and provide all security features to ensure the security of the OptiX OSN 9800 M24/M12/M05 devices.

The UTS is relying on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc.

2.3 Software Architecture

The OptiX OSN 9800 M24/M12/M05 devices are 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, consisting of OTN line board, Optical layer board, Packet board, and TDM board etc.

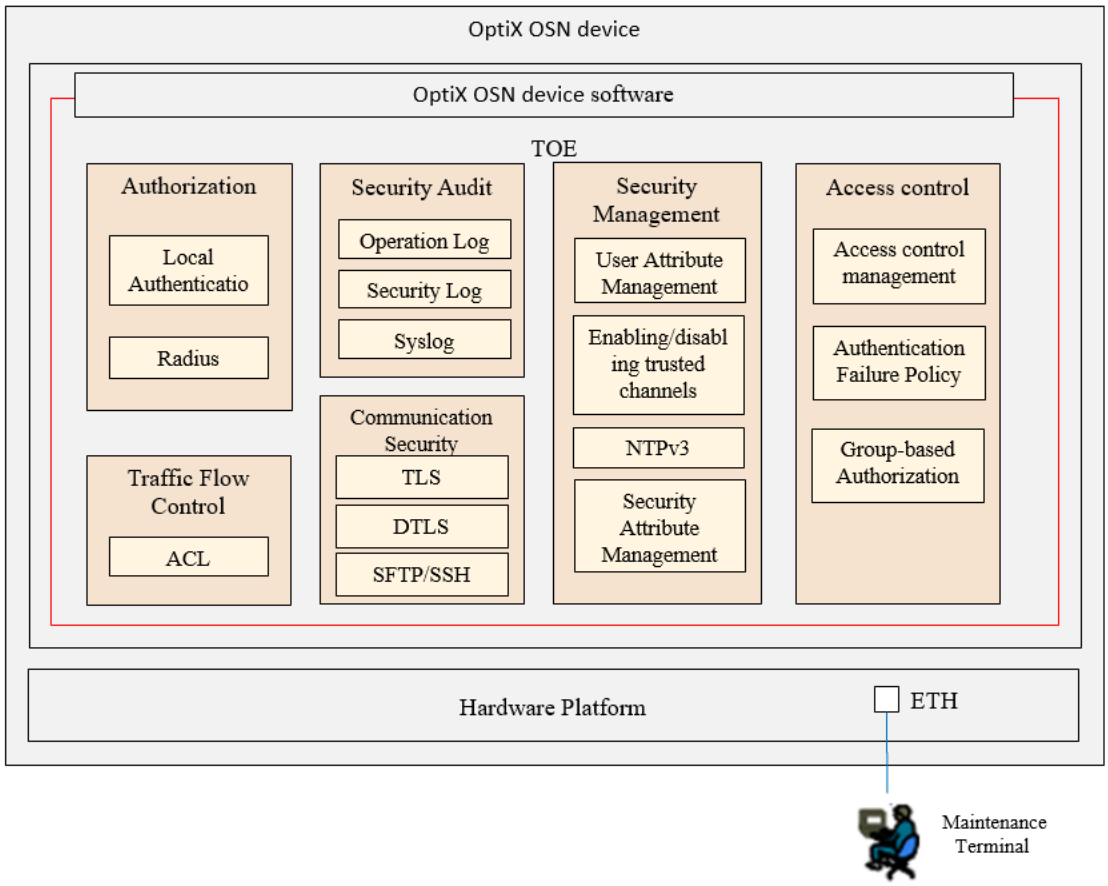
The SCC (System Control and Communication) unit is the center of the system. All service units are centrally managed and controlled by the SCC unit, in which independent control and management software is running.

The software of OptiX OSN 9800 M24/M12/M05 is deployed in the SCC unit and service units, which is responsible for the system management and control and service transmission.

The TOE type is a software, which is part of the OptiX OSN 9800 M24/M12/M05 devices. It consists of the Unified Transmission Software (UTS) component, which is the platform software, and the underlying OS for the System Control and Communication unit as shown in Figure 2-5. These components provide the core control and management services of the device. The TOE is deployed in the SCC unit.

The non-TOE SW components include system and service attribute management, service scheduler and protection, optical Layer protocol, service warning and performance, and service control and monitor.

Figure 2-5 Optix OSN software architecture



The UTS is responsible for managing and controlling the whole OptiX OSN 9800 M24/M12/M05 software, communication, and security features in OptiX OSN 9800 M24/M12/M05. The UTS is relying on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc. Because the UTS provides most of the security feature of the TOE, the elements evaluated in this analysis are the unified transmission software (UTS) and the underlying OS of the OptiX OSN 9800 M24/M12/M05.

To prevent the security threats of OptiX OSN 9800 M24/M12/M05, the unified transmission software (UTS) deployed in SCC unit provides many security measures to mitigate security risks effectively. The main security features are:

1. Identification and authentication of administrative users
2. Authorization
3. Auditing
4. Communication Security

5. Access Control
6. Cryptographic functions
7. Security functionality management

2.4 TOE features

2.4.1 Identification and Authentication

Identification and authentication includes user access, data access and related security management.

In user access, the TOE provides local and remote authentication modes.

In data access, the available LUN is limited by the initiator. Password authentication is supported for connecting to the TOE over a DCN network. Target LUNs on the TOE can be accessed only when the authentication is passed.

In security management, the TOE provides identification and authentication parameters configuration.

- Management of accounts and account attributes, including account credentials
- Management of the account policy, including password length, failure policy, and lockout policy
- Configuration of network services used by the TOE, such as RADIUS.

NOTE

The user authentication method could be modified. Only the administrator can create users and modify user authentication methods.

2.4.2 Authorization

Authorization consists in assigning rights to perform specific task to accounts based a strictly defined policy, ensuring that certain operations can only be performed by explicitly approved accounts.

The OptiX OSN 9800 administrator account is delivered with default credentials. The end user must change the default password on the first login.

2.4.3 Access Control

The TOE supports filtering of incoming access to management interfaces. An administrative user with a proper role can set the IP whitelist to limit access from IP addresses out of the list.

An account can be used for logins within a specific section of a day, namely, the login time. If an account is used beyond its login time, the login request is refused.

2.4.4 Auditing

The TOE generates audit records for security-relevant management actions and stores the audit records in the TOE, or transmits the audit records to syslog server.

2.4.5 Communication Security

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

Secure communication between the TOE and EMS is ensured by TLS protocol.

Secure communication between the TOE and SSH client is ensured by SSH protocol.

The SSH function implemented by Huawei-developed code basic on standard SSH protocol, and the protocol version is SSHv2.

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 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.

2.5 Non-security features

2.5.1 OSN 9800 series

Specifications		9800 M24	9800 M12	9800 M05
Switching capability	Optical	1 to 20-degree reconfigurable optical add/drop multiplexer (ROADM)		
	Electrical	1:1 cross-connect mode: 4.8 Tbit/s ODUk 4.8 Tbit/s OSUflex 4.8 Tbit/s packet services 1.92 Tbit/s VC-4 80 Gbit/s VC-3/VC-12 1:3 cross-connect mode: 10 Tbit/s ODUk 10 Tbit/s OSUflex	N/A	

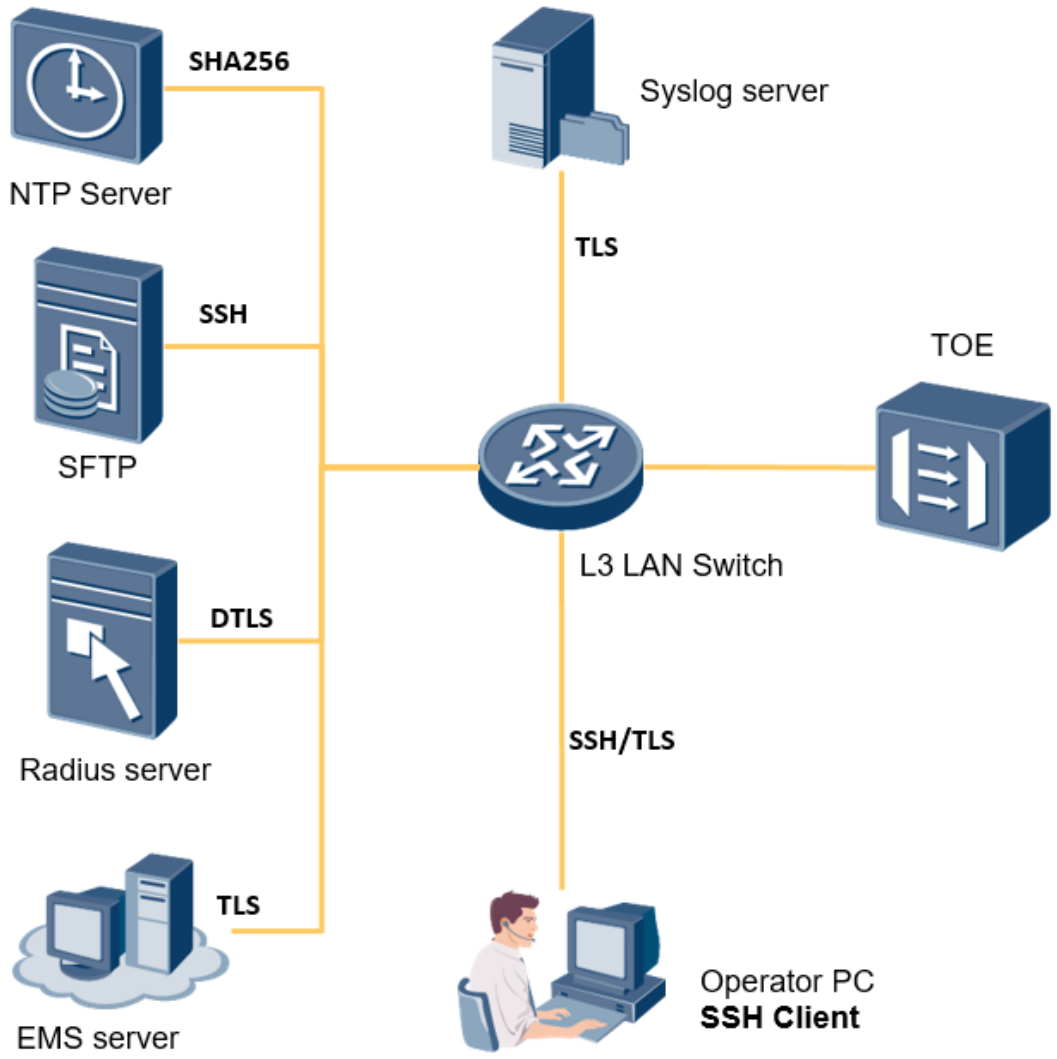
Specifications		9800 M24	9800 M12	9800 M05
		4 Tbit/s packet services 1.6 Tbit/s VC-4 80 Gbit/s VC-3/VC-12		
Max. number of wavelengths		Fixed grid: 120 wavelengths @50 GHz grid Flex grid: The maximum number of wavelengths is related to the width of the flex channel.		
Wavelength range		DWDM system: 1524.50 nm to 1572.06 nm (super C-band) CWDM system: 1471 nm to 1611 nm (S+C+L Band)		
Max. rate per channel		800G bit/s (OTUC8)		
Service type		Synchronous digital hierarchy (SDH)/synchronous optical network (SONET), Ethernet, SAN, OTN, Video		
Packet service capacity		Support E-Line/E-LAN (MEF) and VPWS/VPLS (IETF) Support MPLS-TP Number of MPLS tunnel: 64x1024 Number of PW: 64x1024 Number of E-Line: 32x1024 Number of E-LAN: 8x1024	N/A	
Line rate		2.5Gbit/s, 10Gbit/s, 25 Gbit/s, 100 Gbit/s, 200G bit/s, 400G bit/s, 600G bit/s, 800G bit/s	10Gbit/s, 100 Gbit/s, 200G bit/s, 400G bit/s, 600G bit/s, 800G bit/s	
Supported pluggable optical modules		eSFP, SFP+, TSFP+, CFP, CSFP, CFP2, QSFP28, SFP28, TSFP28, QSFP+, QSFP-DD	eSFP, SFP+, TSFP+, CFP, CSFP, CFP2, QSFP28, SFP28, QSFP+, QSFP-DD	
Topology		Point-to-point, chain, star, ring, ring-with-chain, tangent ring, intersecting ring, and mesh		
Redundancy and protection	Network level protection (OTN)	Optical line protection, Client 1+1 protection, ODUk SNCP, OSUflex SNCP, tributary SNCP, intra-board 1+1 protection, LPT	Optical line protection, Client 1+1 protection, intra-board 1+1 protection, LPT, ODUk SNCP, tributary SNCP	
	Network level protection (Packet)	ERPS, LAG, PW APS/FPS, Tunnel APS, MC-LAG, MC-PW APS, LPT	N/A	
	Network Level Protection (SDH)	LMSP, SNCP, Ring MSP	N/A	

Specifications		9800 M24	9800 M12	9800 M05
	Network level protection (EoS)	LAG, DLAG, LCAS, LPT, STP/RSTP, BPS, PPS	N/A	
	Equipment level protection	Power redundancy, fan redundancy, cross-connect board redundancy, communication control and clock processing unit redundancy	Power redundancy, fan redundancy, communication control unit redundancy, clock processing unit redundancy	
Optical power management		ALS, ALC, IPA, IPA of Raman System, IPC		

2.6 Product Usage

See the section 2.1.

2.7 Production environment



1. The management network port of the TOE device connects to the EMS server, SFTP server, RADIUS server, and Syslog server through a switch.

2. EMS/SSH client manages the TOE-equipped devices...

3. The SFTP server provides the upgrade software package for the TOE security update. The SFTP server must support the SFTP server software.

4. The RADIUS server authenticates the user who accesses the TOE. The TOE forwards the user account and password to the RADIUS server through the RADIUS protocol. The RADIUS server verifies the validity of the user account and password and returns the authentication result to the TOE. The RADIUS server must support the Radius Server software and DTLS protocol.

5. The Syslog server receives the audit logs of the TOE through the Syslog protocol and backs up the audit logs of the TOE to the Syslog server. The Syslog server must support the Syslog Server software and the TLS protocol.

6. A device equipped with TOE may transmit service data from a local end to a remote device through a transport network (Transport Network).

3 TOE Evaluated Configuration

3.1 Test environment

The topology of the test equipment is illustrated below:

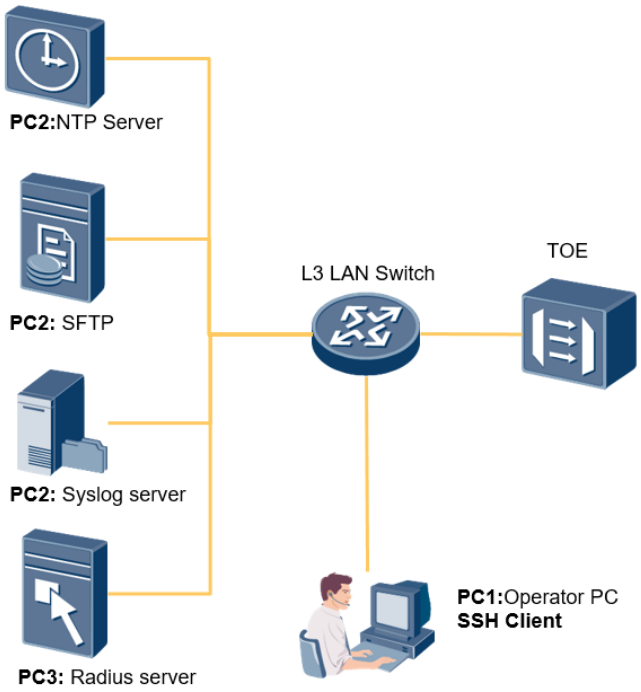


Figure 3-1 Test Environment

- Description

Name	Description	Version	Quantity
TOE	Huawei OptiX OSN device	V100R022C10	1

Test Tools (Simulates services and communicates with TOE devices)

Name	Description	Version	Quantity
NTP	NTP	4.2.8p13	1
SYSLOG	Rsyslogd	8.24.0	1
SFTP	OpenSSH	8.0p1 Debian-4	1
Radius	Free radius	2.2.0	1
OpenSSL	OpenSSL	1.1.1k	1
socat	Socat	1.7.4.3	1

Hardware Test Tools (Test hardware connected to the TOE devices)

Name	Description	Version/OS	Quantity
Switch	Ethernet Switch	N/A	1
PC1	Operator PC/SSH client	OS of windows 10	1
PC2	Support NTP/SFTP/SYSLOG Server	OS of Linux	1
PC3	support Radius Server,support Radius over DTLS	OS of Linux	1

- PC1
  - Hardware
    - ✓ Rack servers or PCs with at least one 100M/1G Ethernet port and one Serial port
  - Software
    - ✓ Windows 10 OS
    - ✓ Brower Google Chrome 64+
    - ✓ Wireshark 3.4.6, notepad ++, Nmap 7.80
- PC2 server
  - Hardware
    - ✓ Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - ✓ OS of Linux
    - ✓ NTP server, SFTP/FTP server, SYSLOG server
    - ✓ Tcpdump
- PC3 server
  - Hardware
    - ✓ Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - ✓ Radius server (support Radius over DTLS)

3.2 Initial configuration

For details about the initial configuration of OptiX OSN device, see the configuration guide "**Huawei OptiX OSN9800 series product Preparative Procedures**".

4 Security Perimeter

4.1 Typical Users

This evaluation requires four user roles to verify the authorization mechanism defined in section 2.4.2, see Table 4-1 Typical user roles. The user group permissions is built on a pyramidal scheme, each user group encompasses the rights attributed to the lower user group: Monitor>Operator>Maintainer>Administrator. Thus the Table 4-1 only display the incremental permission, for futher details see 5.2.

Table 4-1 Typical user roles

User role	Permissions
Monitor level user	Can query the basic attributes of the system and service configurations.
Operator level user	Can configure the basic attributes of the system and service configurations.
Maintainer level user	Can perform basic operations related to the maintenance of the system and services.
Administrator level user	Have full control over the storage system and can manage users.

NOTICE

The same account cannot be used to open several parallel sessions in the meantime.

4.2 TOE Assets

All data available on the TOE is categorized into TSF data and non-TSF data. The following is an enumeration of the subjects and objects participating in the policy.

- **TSF data:**
  - Authentication data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
    - ✓ User identities.
    - ✓ Locally managed passwords.
    - ✓ Locally managed access levels.
  - Audit data: The data which is provided by the TOE during security audit logging.
    - ✓ Audit records.
  - Configuration data for the TOE, which is used for configuration data of security features and functions.
  - Crypto data : cryptographic material used for operations such as digital signature handling and encryption/decryption.

- ✓ X.509 certificates (private keys)

- Management traffic data: communication between authorized user (via the EMS or SSH client) and TOE management interfaces, RSYSLOG server, Radius server, NTP server.

4.3 Threat Model

4.3.1 Threat Agents

The following attackers are considered:

- Attackers without rights for accessing the TOE (i.e., external actor with only means to affect the incoming traffic).
- Unauthenticated User (i.e., actor who manage to get access to the TOE without being authenticated).
- User with restricted actions and authorizations (i.e., privilege escalation attempt).
- Attacker without rights the management network (i.e., intercept and modify traffic between the remote management terminal and the TOE).

4.3.2 Threats

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

- **T.UnwantedManagementTraffic**
  - **Threat agent:** Attackers without rights for accessing the TOE**.**
  - **Asset:** Audit data, Configuration data.
  - **Adverse action**: Disturbance on TOE operation.
- **T.UnauthenticatedAccess**
  - **Threat agent**: Unauthenticated actor.
  - **Asset**: Audit data, Authentication data, Configuration data.
  - **Adverse action**: Illegal access to the TOE.
- **T.CompromisedAudit**
  - **Threat agent:** All threat agents considered in 4.3.1.
  - **Asset:** Audit data
  - **Adverse action:** Compromising of the audit data.
- **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. Malicious update**
  - **Threat agent: Attacker malware package to upgrade software.**
  - **Asset**: Authentication data, Audit data, Configuration data, Crypto data, Management Traffic data.
  - **Adverse action**: use the malware package to upgrade software, modify or replace the TOE software.

- **T.Intercept**
  - **Threat agent**: Remote attacker in the management network.
  - **Asset**: Crypto data, Management Traffic data.
  - **Adverse action**: Intercept, modify and re-use management information assets that are exchanged between the TOE and EMS/SSH client.

4.4 Assumptions

- **A.Certificates**

  It is assumed that digital certificates that are generated externally by trusted certification authorities are of good quality i.e. meeting corresponding standards and providing sufficient security strength through the use of appropriate cryptographic mechanisms and cryptographic parameters. This applies for the cryptographic mechanisms and parameters contained in the certificate and as well for the mechanisms and parameters used to sign the certificate. It is assumed that administrators examine the quality of the certificates besides verifying the integrity and authenticity before importing them. Especially certificates signed with weak hashing algorithms are assumed to be not imported into the TOE.

- **A.PhysicalProtection**

  It is assumed that the TOE and its operational environment (i.e. the complete system including attached peripherals) are protected against unauthorized physical access. It is assumed that only administrators (i.e. all users who could successfully authenticate to the TOE) and non-administrators (i.e. all users who could not successfully authenticate to the TOE) with explicit approval by the administrator(s) are authorized to physically access the TOE and its operational environment. This assumption includes that the local management network, including the RADIUS server, syslog server, NTP server, SFTP servers together with all related communication lines are operated in the same physically secured environment as the TOE. RMT need to be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic means and do not need any physical protection. It is assumed that all RMTs as well as peripherals like RADIUS server, NTP server, SFTP servers or syslog server are connected to the TOE via the same segregated management network (see

also A.NetworkSegregation). As a result, it can be assumed that the TOE and its operational environment are physically protected and are not subject to physical attacks.

- **A.NetworkElements**

  For compatibility reasons, the FTP protocol has not been deleted from the TOE yet, but it is disabled by default. Customers can manually enable FTP due to service requirements. We strongly recommend SFTP ,and provide warnings for using FTP.**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 administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

- **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.

5 TOE Security Functions

5.1 SF.Identification and Authentication

The purpose of authentication and identification is to make sure a user can access the TOE only after the TOE has identified the user identity as the right account.

- The TOE provides local and remote authentication modes
  - In local authentication mode, the user identities are stored locally on the TOE.
    - ✓ The password authentication works based on the comparison between the hash of the input password and the one stored in the TOE.
    - ✓ The password at least contains four types of the following character types: capital letter, small letter, number, and special character (~!@#$%^&*()_+=\|[{}];:'",<.>/? and spaces). The minimum password length can be changed to 8 to 16 characters. The default minimum password length is 12 characters. It is strongly recommended that the set the minimum password length to 16 characters.

      NOTICE

      In CLI scenarios, semicolons(;) is used to separate commands. Therefore, semicolons (;)cannot be used as password characters on the CLI. However, CLI login is not affected.
    - ✓ The cryptographic algorithm of the password of the default user or new added user is PBKDF2.

      Note: To ensure compatibility, if MD5 is used for user encryption on devices of an earlier version on the live network, the system retains the settings of the earlier version after the device is upgraded to the new version. The device reports a risk alarm for the historical account that uses MD5. The administrator needs to change the encryption mode of the historical account to PBKDF2. MD5 is no longer available for new users and initial default users.
  - In remote authentication mode, the user identities are stored in a remote RADIUS server.

- The RADIUS server's essential information (including the IP address, port, and protocol) is configured by a user whose role has the proper permissions. In this type of identification, the TOE acts as a RADIUS client. The input account name and password are forwarded to the RADIUS server through the standard RADIUS protocol and are verified by the RADIUS server.
  - ✓ Remote users are managed by the RADIUS server. However, it is strongly recommended that the password policy of the RADIUS users is the same or stronger than the password policy of TOE.

- Authentication occurs not only in logging in to the TOE, but also in executing some vital commands such as changing one's own password. This is called re-authentication.
- In local authentication mode, if the identification is successful, information about the last successful login (including and time) will be displayed. In remote authentication mode, there is no last login information because all the user information is in the remote server, the remote server and TOE will record login logs.
- No mater any reason the authentication or re-authentication fails with, the TOE will only give blurry feedback to prevent from brute-force cracking. In addition, after the authentication or re-authentication failure, the failure count is recorded in the TOE. After N consecutive authentication failures during 3 minutes, the account will be locked for M minutes, in which N is a positive integer from 1 to 10 and M is a positive integer from 1 to 1000. Both of the values can be configured by a user whose role has proper permissions and both take effect globally.
- After a successful identification, a session will be created to stand for the user dynamically. During the session's creation, a random unique number will be generated as an identifier of the session, and the user's account name, account role and other security attributes will be assigned to the session. A session will be terminated if it is inactive up to N minutes, in which N is a positive number from 5 to 60 and is configured by Administrative Users.

This security function counters the threats: **UnauthenticatedAccess.**

5.2 SF.Authorization

The TOE enforces an access control by supporting following functions in Table 5-2:

- 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. Table 5-1 Groups definition lists the groups and their definition. The accounts of the administrator group are authorized to perform all security management and maintenance operations.

Table 5-1 Groups definition

Group	Permission
Monitor	An account in this group has the lowest permission in the system. He only has the permission to **query** the basic attributes of the system and service configurations and modify the password of the used account.
Operator	An account in this group has a higher permission than a monitor account. He has the permission to **configure and query** the basic attributes of the system and service configurations and modify the password of the used account.
Maintainer	An account in this group has a higher permission than an operator account. It has the permission to configure and query the basic attributes of the system and service configurations, **perform the basic operations of maintaining the system and services**, and modify the password of the used account.
Administrator	An account in this group is a system administrator account. It has the permission to perform **all operations**, such as user management.

When an account is created, it is authorized to perform certain operations and is not allowed to perform others. The access control is achieved by comparing the permissions held by the account's role and the permissions of the operations (i.e. commands). If an account attempts to perform any unauthorized operation, the attempt is audited.

- 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 5-2.
- Every management command has a command level associated to it. A user can use this command if his user level dominates the command level, i.e., if his user level is hierarchically equal or higher than the command level. User groups match to command levels as follows:

Table 5-2 Correspondence of user groups and command levels

User group	User group map to CLI	Command Level
Monitor	Every	Monitor
Operate	Oper	Monitor Operate
Maintenance	Maint	Monitor Operate Maintenance
Administrator	Admin	Monitor Operate Maintenance

		Manage Debug

NOTICE

Each user account can run the ‘:help’ command to query the commands that can be executed by the current user permission level.

- In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user level and cannot increase the user level attribute beyond their own user level. Command levels cannot be changed by users.

This security function counters the threats: **UnwantedManagementTraffic, CompromisedAudit, and UnauthorizedAccess.**

5.3 SF.Access Control

Access control list (ACL) can be used for basic traffic filtering. ACL can be configured for all the NEs to filter IP packets that have been received. Devices support basic, advanced, L2 ACL rules.

Note：
Pay attention to using the command to set the ACL, because wrong setting of the ACL may cause to fail to log in to an NE.

Basic ACL Rules
For ordinary TOEs that do not have high security requirements, can use the basic ACL rules. The basic ACL rules examine the source IP addresses of the received packets. The basic ACL rules do not use many system resources.

Advanced ACL Rules
For TOEs that have very high security requirements, can use advanced ACL rules. The advanced ACL rules examine the source and sink IP addresses, the source and sink port IDs, and the protocol types of the received IP packets. The implementation of advanced ACL rules uses many system resources. The advanced ACL rules have higher priority than the basic ACL rules.

L2 ACL Rules（Link-layer ACL）
The L2 ACL rules examine the source and sink MAC address of incoming packets. ARP Filter Type use to set whether only to filter the ARP packet.

Firewall ACL Rules（Interface-based ACLFW rules）
For NEs that require interface-level filtering, you can set Firewall ACL rules. A Firewall ACL rule checks the source and destination addresses, source and destination ports, and protocol type of IP packets received by the interface bound to the rule. If both Firewall ACL and ACL rules are configured, the system preferentially uses the Firewall ACL rule for verification.

NOTICE

The priority of an ACL rule is as follows: Firewall ACL Rules > L2 ACL rules > advanced ACL rule > basic ACL rule. ACLs are matched according to the order of the rule number from small to large. When a rule is matched, it will stop matching and process it according to the operation type of the rule, allowing or prohibiting it. If it does not match, it will go to the next rule. If there is no match, the packet is allowed.

This security function counters the threats: UnwantedManagementTraffic, **UnauthenticatedAccess.**

5.4 SF.Audit

From the perspective of security, the system provides the security log and operation log. Those two logs will be send to a syslog server if one is configured.

The security log records operations about account management, such as changing passwords and adding accounts. The operation log records activities about system configurations, such as modifying the device IP address and adding services

- Operation log

Non-query operations and the operations of querying sensitive information are recorded in the operation log, including the account name, terminal address, operation time, operations, and operation results.

- Security log

The security log tracks security-related configuration operations, including user management, security settings, user logins and logouts, and the attempts of unauthorized operations. The security log provides the information about the account name, address of the client, time, and operation.

The TOE provides an audit trail for all essential operations.

- All non-query operations will be recorded in the operation logs. Typically, these operations include login, logout, configuration change, user management, and security settings.
- An audit record is composed of 6 basic items: who (user name), where (user IP address), when (timestamp), what (operation description), result (success or specific error code), and ID (a unique number of this record).
- Review functionality is provided via the EMS/SSH client, which allows Administrative Users to inspect the audit logs. Administrative Users can query or fetch the audit trail.
- All audit trails are stored locally in the TOE's persistent media. An SFTP/FTP server to dump audit records can be triggered via EMS/SSH client by Administrative Users. If such an SFTP/FTP server dumping operation is not issued, the newer records will overwrite the oldest stored audit records once the log-file is full.
- All audit trails are securely transmitted to syslog server for centralized log management, if a syslog server is configured and the transmission is enable. If the SYSLOG_COMM_FAIL alarm is generated, which means the TOE and the SYSLOG server have an abnormal

connection and the audit logs of the TOE cannot be sent to the SYSLOG server, the maintenance engineer must restore the connection between the TOE and the SYSLOG server, and query or upload the security logs and operation logs from the TOE to ensure the integrity of audit data.

- The NTP service can synchronize all the clocks of devices on the network so that these devices can provide audit trails' timestamp with the uniform time. The NTP authentication algorithm supports HMAC-SHA256 and MD5. Users are advised to use the secure hmac-sha256 algorithm. But for compatibility, user can use the md5 algorithm. When MD5 is enabled, the system will notice the user that the NTP uses an insecure algorithm.
- The TOE supports manual export of security logs and operation logs using SFTP.
- Audit records are protected against malformed inputs, which can compromise their integrity.

This security function counters the threats: **CompromisedAudit.**

5.5 SF. Communication Security

The TOE provides communication security by implementing trusted channels between the EMS as server, and acts as client during the TLS communication established between the TOE and Syslog server.

The TOE is using the TLS communication protocol. The TLS1.2 and TLS1.3 protocol are implemented to provide communication channels. The TOE acts as a TLS server and allows other trusted IT products to initiate communication. TLS certificates are required for establishing TLS encryption channels. The TLS certificates for server authentication are managed and issued by users. The TOE supports TLS certificate loading and activation. SFTP (description as below) is used to load TLS certificates onto TOE before establish TLS communications. The TOE acts as server during the TLS communication established between the TOE and EMS, that is to say, the EMS will validate the certificate from the TOE. The TOE does not provide path validation capabilities for X.509 certificates.

Client authentication is performed password-based on the application layer. The TOE has been loaded with a preset TLS certificate before delivery. If the below-mentioned TLS_RSA ciphers are used, the RSA public key is used for authentication and key exchange. Using the below TLS_DHE ciphers the standard Diffie-Hellman parameters P and G.

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 SSH server and SFTP client which initiates communication with other trusted IT products.

The TOE SSH server supports password authentication and key authentication. The SSH server generate an RSA key for the client to authenticate the server, The length of the RSA key ranges from 2048 to 4096 bits and is specified by users.

When the SSH server private key is generated, the TOE generates a random password through secure random number to protect the private key security.

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 RSA key. For the key authentication, users need to generate the RSA key on the TOE first and upload the public key to the SFTP server. The length of the RSA key ranges from 2048 to 4096 bits and is specified by users.
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.

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.

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.

This security function counters the threats: T.**Intercept.**

5.6 SF.Trusted Update

Only authenticated administrators have the ability to manually initiate an update to TOE firmware/software. During the updating procedure, digital signature will be verified by the TOE at first. Using SFTP as the secure transmission channel for the upgrade.
The administrators can query the currently executing version of the TOE firmware/software by a command. The currently executing patches and most recently installed patches can also be checked out.
The validation of the firmware/software integrity is always performed before the process of replacing a non-volatile, system resident software component with another is started. All discrete software components (e.g. applications, drivers, kernel, and firmware) of the TSF are archived together into a whole package and the single package is digitally signed.
This security function counters the threats: **Malicious update.**

6 Rationale

6.1 Assets vs security needs

The following security needs of assets are:

		Availability	**Confidentiality**	**Integrity**
TSF data	Authentication data	X	X	X
	Audit data	X	X	X
	Configuration data	X	X	X
	Crypto data	X	X	
	Management traffic data	X	X	X

6.2 Assets vs Threats

Threat Asset	T. UnwantedManagementTraffic	T.UnauthenticatedAccess	T.CompromisedAudit	T.UnauthorizedAccess	**T. Malicious update**	T. Intercept
Authentication data		I		Av, I, C	Av, I	
Audit data	Av	I, C	Av, I	Av, I, C	Av, I	
Configuration data (TSF)	Av	Av, I, C		Av, I, C	Av, I	
Crypto data				Av, I, C	Av, I	I, C
Management traffic data				Av, I, C	Av, I	Av, I, C
		Av: Availability, I: Integrity, C: Confidentiality				

6.3 Threats vs security functions

Threat Security Function	T.Unwanted Management Traffic	T.UnauthenticatedAccess	T.CompromisedAudit	T.UnauthorizedAccess	**T. Malicious update**	T. Intercept
SF.Identification and Authentication		X				
SF.Authorization	X		X	X		
SF.Access Control	X	X				

SF.Audit			X			
SF.Communication security						X
SF.Tursted Update					X	