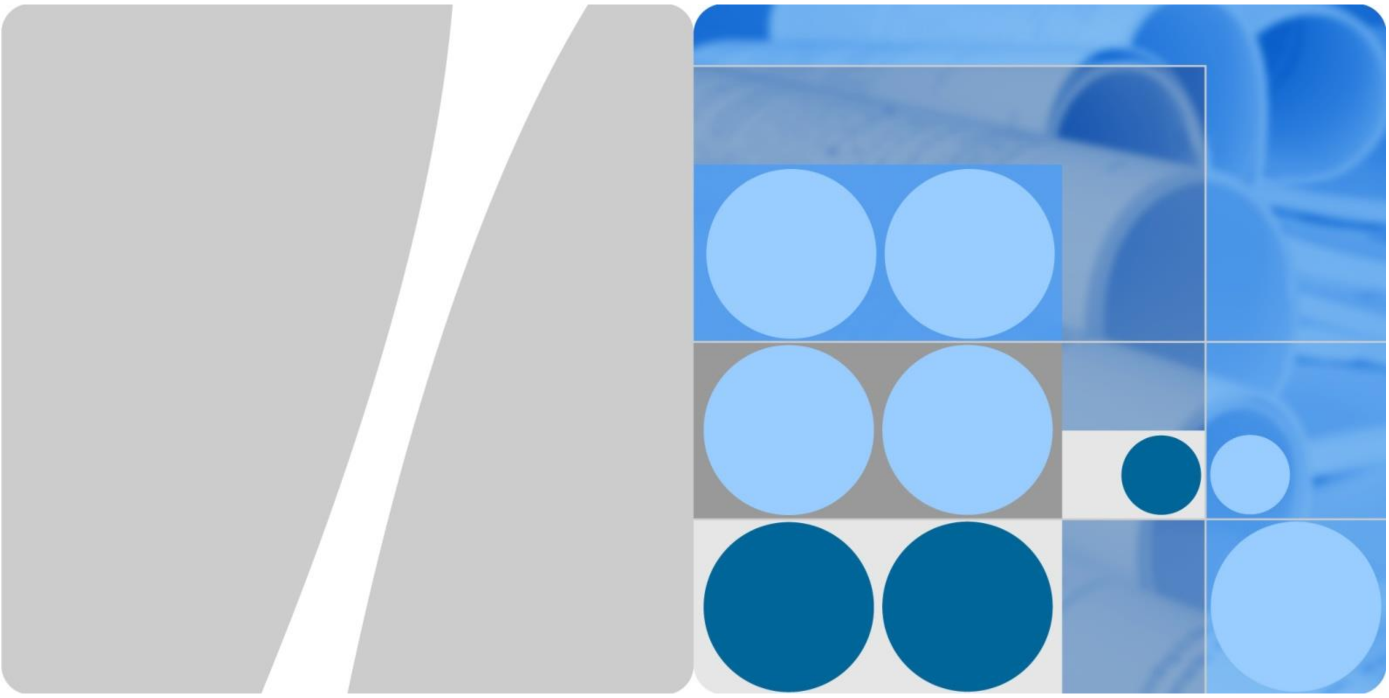


Huawei OptiX OSN9800&OSN1800 V100R021 C10 Software Security Target

Issue	1.4
Date	2023-09-11

HUAWEI TECHNOLOGIES CO., LTD

Trademarks and Permissions

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 (U64E/U32E/M24/M12/M05) and Optix OSN1800 (OSN1800 II Pro、OSN1800 II TP、OSN1800 V、OSN1800 V Pro)series product software management component, consisting of unified transmission software (UTS). The software is part of OptiX OSN 9800 (U64E/U32E/M24/M12/M05) and Optix OSN1800 (OSN1800 II Pro、OSN1800 II TP、OSN1800 V、OSN1800 V Pro)series product.

Symbol Conventions

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

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠ NOTICE	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.
🕮 NOTE	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.

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
2022-8-22	1.0	Initial Draft	Diao Runan ,Zhou Jie
2023-2-23	1.1	Modified based on review comments	Diao Runan
2023-6-19	1.2	Modified based on review comments	Diao Runan
2023-07-05	1.3	Modified based on review comments	Diao Runan
2023-09-11	1.4	Correct guidance version	Diao Runan

content

1 Introduction

This Security Target is for the evaluation of OptiX OSN 9800 series (U64E/U32E/M24/M12/M05) and OptiX OSN 1800 series (OSN1800 II Pro、OSN1800 II TP、OSN1800 V、OSN1800 V Pro) software, consisting of unified transmission software (UTS). The software is part of OptiX OSN 9800 series and 1800 series.

Unless otherwise specified, OSN Series is used to replace the OptiX OSN 9800 and OptiX OSN 1800 series.

1.1 ST Identification

Title: Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software Security Target

Version: 1.4

Date: 2023-09-11

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software

Version: V100R021C10SPC300

Developer: Huawei Technologies Co., Ltd.

VRC versions are defined as follows:

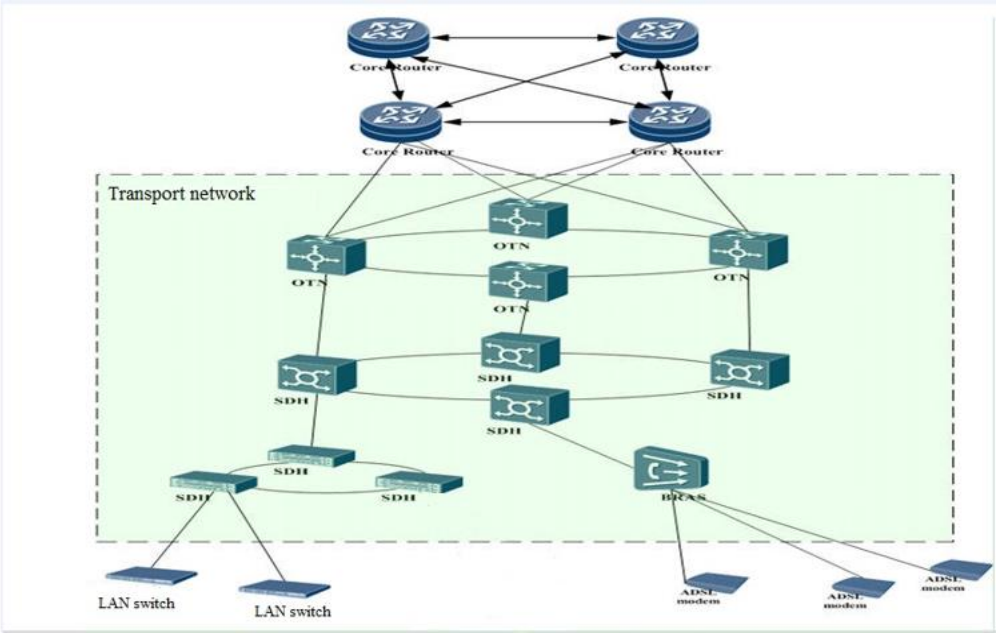
- V version is the version of the software or hardware platform that a product bases.
- R version is released for customer at a specific time. It is a collection of features that is embodied in the form of a product.
- C version is the customized version developed based on the R version to fast meet 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 access layer of the network,
- the metro or aggregation layer of the network,
- the core or backbone core layer of the network.

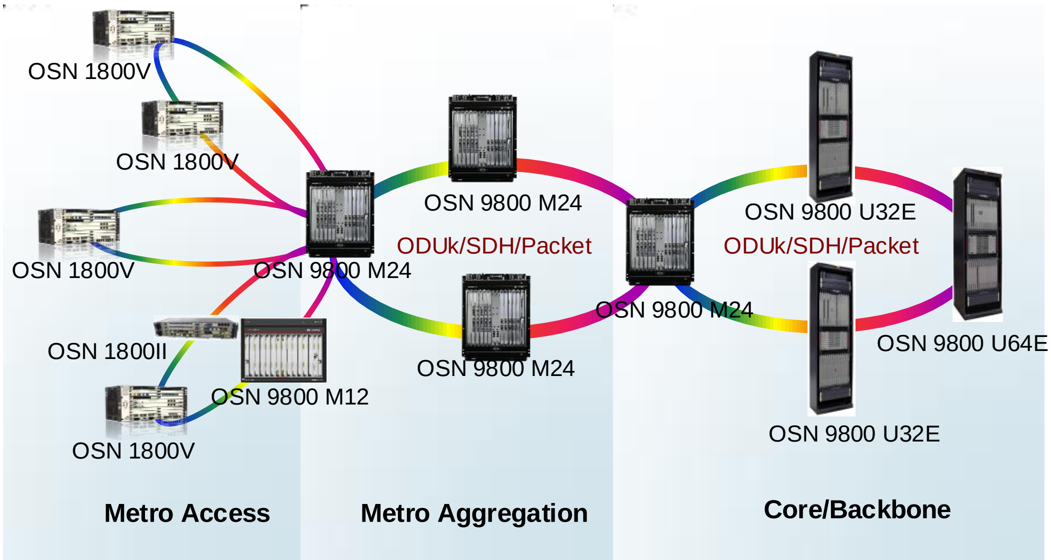
The access layer of the network is mainly responsible for the access control of the services of individual and enterprise users. The metro or aggregation layer of the network is to converge the massive user traffic and connect the access layer and backbone or core layer of network. The role of the backbone 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 OSN Series device is 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 1-2. 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 OSN Series device works with the current OptiX WDM equipment to extend the services to the access layer.

OSN 9800 M24 subrack is a next-generation large-capacity OTN product that integrates ASON (Automatically Switched Optical Network), OTN, and packet functions. It is applicable to various networks, including super-backbone, backbone, and metro networks.

OSN 9800 M24&M12 and OSN 1800 subrack is a next-generation ultra-large capacity, high integration, and optoelectronic OTN/WDM product developed based on new software and hardware platforms. It is applicable to backbone and metro networks.

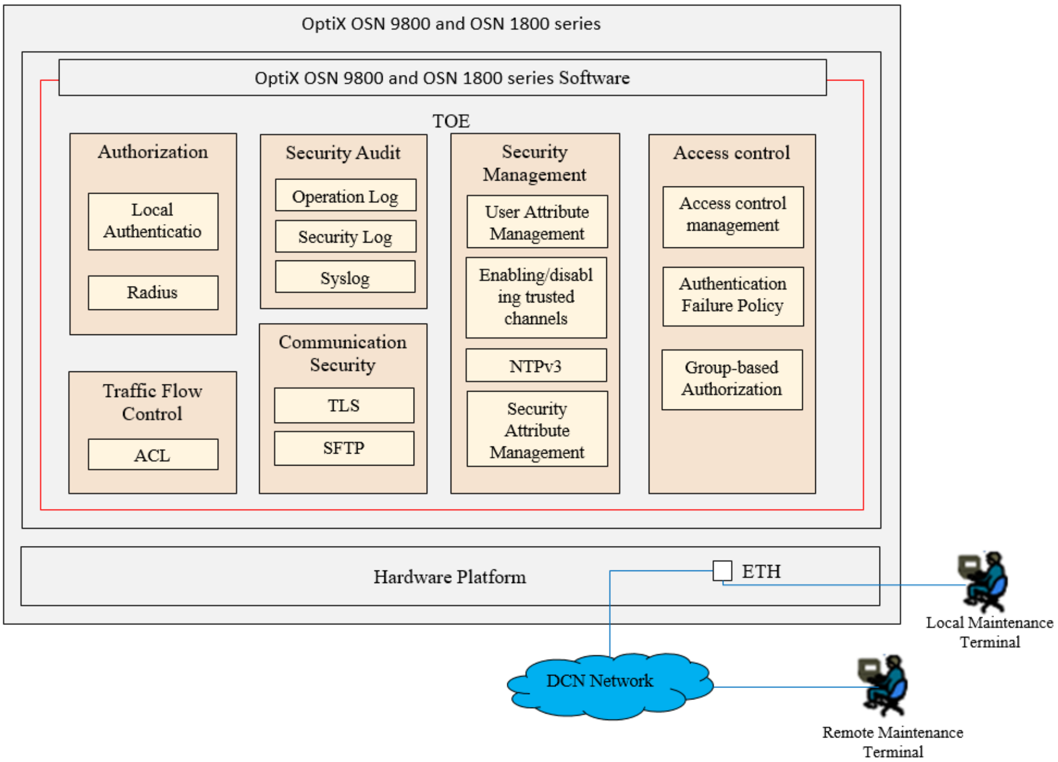
Figure 1-2 Position of the OSN Series on the entire network



1.4 TOE Overview

The TOE is the OSN Series software which contains Unified Transmission Software (UTS) and for the System Control and Communication as shown in Figure 1-3. It provides the core control and management services of the device.

Figure 1-3 TOE constitution


OptiX OSN 9800 and OSN 1800 series
OptiX OSN 9800 and OSN 1800 series Software
TOE
Authorization
Local Authenticatio
Radius
Security Audit
Operation Log
Security Log
Syslog
Security Management
User Attribute Management
Enabling/disabling trusted channels
NTPv3
Security Attribute Management
Access control
Access control management
Authentication Failure Policy
Group-based Authorization
Traffic Flow Control
ACL
Communication Security
TLS
SFTP
Hardware Platform
ETH
Local Maintenance Terminal
DCN Network
Remote Maintenance Terminal

The TOE is responsible for managing and controlling the whole OSN Series software, communication, and security features in OSN Series.

To counter the security threats of OSN Series, the TOE provides 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. Management Traffic Flow Control
6. Security functionality management

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

1.5 TOE Description

1.5.1.1 Physical scope

The TOE is 'software only'. The TOE consists of the software of the OSN Series, but not the hardware, which the TOE is running on. The customer need to download the software package as well as the guidance documents as pdf files from Huawei’s support website (https://support.huawei.com) and the user has to verify the signature values given in the Table 1-1 below for all TOE parts for secure acceptance.

Table 1-1 Delivery Items

Type	Delivery Item	Version
Software	OptiX OSN 9800 U32E_V100R021C10SPC300.zip OptiX OSN 9800 U64E_V100R021C10SPC300.zip	V100R021C10SPC300
	OptiX OSN 9800 M24_V100R021C10SPC300.zip OptiX OSN 9800 M12_V100R021C10SPC300.zip OptiX OSN 9800 M05_V100R021C10SPC300.zip	
	OptiX OSN 1800 V Pro_V100R021C10SPC300.zip OptiX OSN 1800 II Pro_V100R021C10SPC300.zip OptiX OSN 1800 II TP_V100R021C10SPC300.zip OptiX OSN 1800 V_V100R021C10SPC300.zip	
Software Signature File	OptiX OSN 9800 U64E_V100R021C10SPC300.zip.asc OptiX OSN 9800 U32E_V100R021C10SPC300.zip.asc	V100R021C10SPC300
	OptiX OSN 9800 M24_V100R021C10SPC300.zip.asc OptiX OSN 9800 M12_V100R021C10SPC300.zip.asc OptiX OSN 9800 M05_V100R021C10SPC300.zip.asc	
	OptiX OSN 1800 V Pro_V100R021C10SPC300.zip.asc OptiX OSN 1800 II Pro_V100R021C10SPC300.zip.asc OptiX OSN 1800 II TP_V100R021C10SPC300.zip.asc OptiX OSN 1800 V_V100R021C10SPC300.zip.asc	
Product Guidance	OptiX OSN 9800 Intelligent Optical Transport Platform V100R021C10 Product Description https://support.huawei.com/hedex/hdx.do?docid=DOC1100930606&id=EN-US_TOPIC_0000001153273528	issue 04
	OptiX OSN 1800 Intelligent Optical Transport Platform V100R021C10 Product Description https://support.huawei.com/hedex/hdx.do?docid=DOC1100931171&id=EN-US_TOPIC_0000001225866818	issue 04
	Huawei OptiX OSN9800&OSN1800 V100R021C10 Software - AGD_OPE	V1.1, 2023-07-05
	Huawei OptiX OSN9800&OSN1800 V100R021C10 Software - AGD_PRE	V1.3, 2023-07-05
	Huawei OptiX OSN9800&OSN1800 Software Configuration and Reference	V1.0, 2022-08-21

1.5.1.2 Logical scope

- **Identification and authentication**

The TOE can authenticate administrative users by user name and password.

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 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 EMS sessions via TLS sessions. The use of TLS connection is always required for accessing the TOE via RMT. For LMT no logically secured communication channel is required.

- ## 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 commands 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. All authenticated users of the TOE are administrative users of some kind belonging to one of the user groups defined below. There are no authenticated non-TOE administrative users.

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.

- ## 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.

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.

- **Communication Security**

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

For the secure communication between the TOE and the EMS the TLS protocol is used. TLS1.2 and TLS1.3 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')). 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.

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 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.

- **Management 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.

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. The protocol features include source port of the TCP protocol, destination port of the TCP protocol, and ICMP protocol type.

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.
Sink IP address	Sink IP address	The destination IP address and the sink wildcard determine the addresses to which an access control rule is applicable.
Sink 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**.

Parameter	Value Range	Description
Sink 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.

- **Security functionality 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
- 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 level for execution.

1.5.2 Non-TOE Hardware and Software

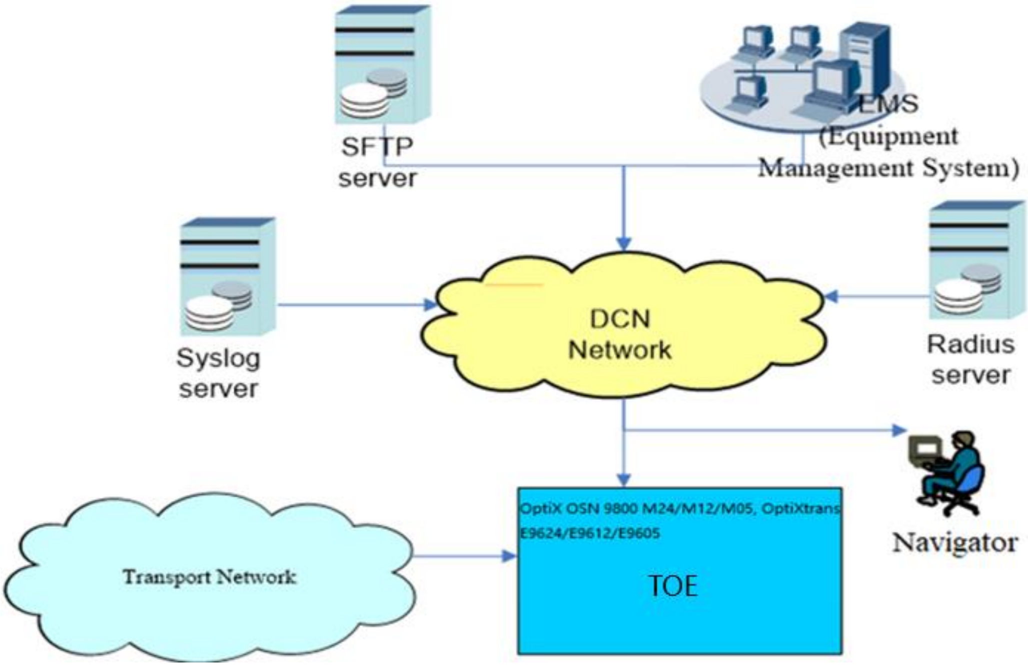
Based on physical scope and logical scope described so far, a list of configuration is to be added:

- For management via the ETH interface, authentication is always enabled. Authentication mode is username and password or Authentication, Authorization, Accounting ('AAA', i.e. username and password). Length of password is no less than 12 characters.
- Service of FTP have to be disabled to use the TOE in the certified configuration.

The environment for TOE comprises the following components as shown in figure 1-4:

- Local PCs (WebLCT) used by administrators to connect to the TOE for access through interfaces on SCC unit via a secure channel of TLS, or non-secure channel. Access will be performed using a command line terminal.
- Remote PCs used by administrators to connect to the TOE for access through interfaces on SCC unit within the TOE via a secure channel of TLS.
- EMS (Element Management System), it typically runs the NCE rich user interface management software.
- SFTP Server is a light-weight high performance SSH File Server and make configuration simple.
- Radius server is optional and may be used instead of local authentication.
- Syslog server is optional and is used for receiving audit information from the TOE via SYSLOG protocol.
- NTP server is used for synchronizing time to the TOE.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- OSN Series hardware, include BIOS/FPGA/CPLD of SCC board:
    - OptiX OSN 9800 series hardware: U64E/U32E/M24/M12/M05
    - OptiX OSN 1800 series hardware: OSN1800 II Pro、OSN1800 II TP、OSN1800 V、OSN1800 V Pro

Figure 1-4 The TOE in its operational environment



2 CC Conformance Claims

2.1 CC Conformance Claim

This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC]. The CC version of [CC] is 3.1R5.

The ST claims conformance to the EAL4 augmented with ALC_FLR.2.

No conformance to a Protection Profile is claimed.

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 EMS from authorized users.

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 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 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 A remote attacker is able to intercept, modify and re-use management information assets that are exchanged between the TOE and EMS or WebLCT. This comprises Authentication data (in particular authentication data of administrative 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 exchanged between the TOE and a trusted IT product. 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: Remote attacker in the management network.

  Asset: Authentication data, Crypto data, Configuration data.

  Adverse action: Intercept, and potentially modify or re-use information that are exchanged between TOE and EMS or WebLCT.

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.

3.4 Assumptions

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

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) 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 and locally attached management terminals (LMT) together with all related communication lines are operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) 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 It is assumed that the operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. These network devices are deployed in an independent network which is segregated from other network by VPN or firewall or other methods. Examples of such devices are:

- Peer router(s) for the exchange of dynamic routing information;
- Local and remote management terminals (WebLCT, EMS) used for administration of the TOE.
- RADIUS servers for obtaining authentication and authorization decisions.
- SYSLOG servers for receiving and storing audit data.
- NTP servers.

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 (i.e. all users that can successfully authenticate to the TOE) 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.Device It is assumed that the underlying hardware of OSN Series, which is outside the scope of the TOE, as well as the firmware and the underlying OS and non-TOE software, are trusted and works correctly.

A.UpToDateClient It is assumed that the user uses a secure remote management terminal for remote administration of the TOE which is up to date with respect to supported cryptographic algorithms and security measures.

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 to provide functionality generate audit records for security-relevant administrator actions.
- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and RMT as well as the TOE and trusted IT products from the operational environment.
- **O.SecurityManagement** The TOE shall provide functionality to manage security functions provided by the TOE.

4.2 Security Objectives for the Operational Environment

- **OE.Certificates** Digital certificates that are generated externally by trusted certification authorities shall be 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. Administrators shall examine the quality of the certificates besides verifying the integrity and authenticity before importing them. Especially certificates signed with weak hashing algorithms shall not be imported into the TOE.
- **OE.PhysicalProtection** The TOE and its operational environment (i.e. the complete system including attached peripherals) shall be protected against unauthorized physical access. Only administrators (i.e. all users who could successfully authenticate to the TOE) shall be authorized to physically access the TOE and its operational environment. The local management network, including the RADIUS server, syslog server, NTP server, SFTP server and locally attached management terminals (LMT) together with all related communication lines shall be operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) shall 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 physically protection. All RMTs as well as peripherals like RADIUS server, NTP server, SFTP server or syslog server shall be connected to the TOE via the same segregated management network (see also OE.NetworkSegregation). As a result, the TOE and its operational environment shall be physically protected and shall not be subject to physical attacks.

- **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 EMS used for TOE management, Syslog servers, SFTP servers, NTP servers and Radius servers for obtaining authentication and authorization decisions.
- **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 administrators (i.e. all users that can successfully authenticate to the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users shall be competent, and not careless or willfully negligent or hostile, and shall follow and abide by the instructions provided by the TOE documentation. All user management and permission management are implemented in the TOE.
- **OE.Device** The underlying hardware of OSN Series, which is outside the scope of the TOE, as well as the firmware and non-TOE software, shall work correctly.
- **OE.UpToDateClient** The user shall use a secure remote management terminal for remote administration of the TOE which is up to date with respect to supported cryptographic algorithms and security measures.

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 OE.NetworkSegregation	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 level (O.SecurityManagement). An independent local network is used to manage the TOE. (OE.NetworkSegregation)

Threat / OSP	Security Objectives	Rationale for Security Objectives
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 level (O.SecurityManagement). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).
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 levels) can be configured by users with sufficient user level (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 EMS and the TOE 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 level (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)

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. Certificates is upheld by OE.Certificates, 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.

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

Table 4-2 Mapping objectives for the environment to assumptions

Environmental Objective	Threat /Assumption
OE.Certificates	A.Certificates
OE.PhysicalProtection	A.PhysicalProtection
OE.NetworkElements	A.NetworkElements
OE.NetworkSegregation	A.NetworkSegregation T.UnwantedManagementTraffic
OE.NoEvil	A.NoEvil
OE.Device	A.Device
OE.UpToDateClient	A.UpToDateClient

5 Security Requirements for the TOE

5.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement

- (underlined text in parentheses) 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 indicates an element of the iteration, where Identifier distinguishes the different iterations.

5.2 Security Functional Requirements

5.2.1 Security Audit (FAU)

5.2.1.1 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:

ii. user management

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

Application Note: Changes to user levels are covered by c.ii.3. user group level change. Command levels are fixed and cannot be modified. 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)**, **User Name (if applicable).**

Application Note: The term ‘if applicable’ shall be read as ‘whenever an event can be associated with the specified information’. For example, if an event can be associated with a User ID, then the event shall be audited and the audit information shall contain the User ID. If the event cannot be associated with the User ID, the event shall be audited and the audit information shall not contain User ID information. If multiple conditional information can be associated with an event (e.g. interface and User ID can be associated with an event), all the conditional information shall be contained in the audit information when auditing the event.

5.2.1.2 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.

5.2.1.3 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.

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

5.2.1.4 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.

5.2.1.5 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.

5.2.1.6 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.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.1 Subset Access Control

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

Subject: user session;

Objects: commands provided by TOE;

Operation: Execute

5.2.2.2 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:

- **user Identity**
- **user level**

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 access to commands.**
2. **Users can be configured with different user group to control the device access permission.**
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 run all commands from the command level corresponding to his user level below.**

User group	Command Level
Monitor	Monitor
Operate	Monitor Operate
Maintenance	Monitor Operate Maintenance
Administrator	Monitor Operate Maintenance Manage Debug

5. **The command level is stored by the TOE (i.e. UTS software) 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.**

5.2.2.3 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. 5.2.2.4).

5.2.2.4 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 attributes: IP address (i.e. IP address setting of the device management interface), Port number

Information security attributes: Source IP address, Destination IP address, IP Protocol number, Source port number, Destination port number

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. **The TOE uses the Access Control List(ACL) to match the IP packets received from the device management interface. If the IP packet match an ACL rule, the TOE discards or accepts the packets based on the action specified in the ACL rule.**
2. **An ACL rule contains one or more of the following attributes: source IP address, destination IP address, IP protocol number, source port number, and destination port number.**

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.**

5.2.3 Identification and Authentication (FIA)

5.2.3.1 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 within certain period of time occur related to **user logging in**.

Application Note: The maximum unsuccessful authentication attempts is 5 by default, the administrator can set it to a value ranging from 1 to 10.

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

1. lock the offending user ID;

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.

5.2.3.2 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. user ID

2. user validity period

3. user level

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

5.2.3.3 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.

5.2.3.4 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 via EMS;

2. Local Authentication by local database of the TOE for authentication via LMT and EMS

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 user id and password).

Application Note: The TOE can use only one of the mechanisms at any given time. The Administrator can configure which mechanism is used by the TOE.

5.2.3.5 FIA_UID.2 User identification before any action

FIA_UID.2.1The 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.

5.2.4 Security Management (FMT)

5.2.4.1 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 administrator user level as defined in FMT_SMR.1**.

5.2.4.2 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 **NTP server address, SYSLOG server address, RADIUS server address, SFTP server address, and Attributes identified in FDP_ACF.1 and FIA_ATD.1** to the **users with administrator user level as defined in FMT_SMR.1**.

5.2.4.3 FMT_MSA.1/IFF Management of Security Attributes

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

5.2.4.4 FMT_MSA.3/ACFATD Static Attribute Initialization

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

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

5.2.4.5 FMT_MSA.3/IFF Static Attribute Initialization

FMT_MSA.3.1/IFF The TSF shall enforce the **Management Network Filtering SFP (based on ACL)** 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 administrator user level as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

5.2.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions (using administrator accounts):

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**

5.2.4.7 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 their own attributes.
Operator	The accounts of this group are authorized to query the system information and perform non-SFRs 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.

5.2.5 TOE access (FTA)

5.2.5.1 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.**

5.2.5.2 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

5.2.6 Trusted Path/Channels (FTP)

5.2.6.1 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).

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

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

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

FTP_ITC.1.3/TLS The TSF shall initiate communication via the trusted channel for **protecting management communication**.

Application Note: The TSF do not initiate any TLS-based communication, but offers the ability for protected communication for users sessions.

5.2.6.2 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].

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].
- Key exchange is performed using diffie-hellman-group14-sha1
- The public key algorithm of the SSH transport implementation is ssh-rsa.

- For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported.
- For data integrity protection HMAC-SHA256, HMAC-SHA512 are supported.

5.3 Security Functional Requirements Rationale

5.3.1 Coverage

As shown Table 5-1 provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 5-1 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
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
FIA_UAU.5	O.Authentication
FIA_UID.2	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
FTA_SSL.3	O.Authentication O.Communication
FTA_TSE.1	O.DataFilter O.Authentication O.Communication
FTP_ITC.1/TLS	O.Authentication O.Communication
FTP_ITC.1/SFTP	O.Authentication O.Communication

5.3.2 Sufficiency

As shown Table 5-2 provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Table 5-2 SFR sufficiency analysis

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 the external NTP server and user identities as defined in FAU_GEN.2 where applicable. 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.
O.Communication	Communication security is implemented by the establishment of a trusted channel for remote users 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.
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. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1. User authentication via RMTs requires the use of 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.
O.Authorization	User identification is addressed in FIA_UID.2. 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. 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.

5.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL4 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 5-3 demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Table 5-3 Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	The TOE relies on the external NTP server to provide the timestamp.
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
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3/ACFATD	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/IFF	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
FMT_MOF.1	FMT_SMR.1	FMT_SMF.1 FMT_SMR.1

Security Functional Requirement	Dependency	Resolution
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
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

5.4 Security Assurance Requirements

The security assurance requirements for the TOE are the EAL4 augmented with ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

5.5 Security Assurance Requirements Rationale

The EAL4 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 (EAL4) 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.

6 TOE Summary Specification

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

6.1 Authentication

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

- Support authentication via local passwords. This function is achieved by comparing user information input with pre-defined user information stored in the flash. Passwords have a length of 12 to 16 characters. The TOE enforces a password complexity policy of at least contains all types of the following character types: capital letter, small letter, number, and special character.
- Support authentication via the remote RADIUS authentication server. The TOE hands identification and authentication information provided by the user during login to the RADIUS server and enforces the RADIUS server’s pass/fail decision.
- Support authenticated user logins using the TLS mode.
- 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.
- Support maximum attempts for authentication failures within certain period of time. By default, after five consecutive 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. A series of whitelists and blacklists are set to filter IP addresses and data on ports. Unauthorized IP addresses and communication ports cannot access the system.
- Support for user individual attributes including the user ID, user level, and password to ensure that each user is unique in the system. Both the user ID and password have a validity period, the user cannot log in to the system If the validity period expires.
- Using the SFTP application requires Administrator users to unlock the private RSA 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. The passphrase complexity requirements are the same as for user passwords.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FTA_TSE.1, FTA_SSL.3)

Table 6-1 SFR to TSF mapping

SFR	TSF
FIA_AFL.1	Support maximum attempts for authentication failures within certain period of time. By default, after five consecutive 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	Support authentication via local passwords. This function is achieved by comparing user information input with pre-defined user information stored in the flash. Passwords have a length of 12 to 16 characters. The TOE enforces a password complexity policy of at least contains all types of the following character types: capital letter, small letter, number, and special character. Using the SFTP application requires Administrator users to unlock the private RSA 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 passphrase complexity requirements are the same as for user passwords. Support for user individual attributes including the user ID, user level, and password to ensure that each user is unique in the system. Both the user ID and password have a validity period, the user cannot log in to the system If the validity period expires.
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. The TOE provides two session establishment mechanisms requiring identification and authentication of users: via MML commands for file uploads and downloads over SFTP and via QX commands for all other administrative activities.
FIA_UAU.5	Support authentication via local passwords. 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 identification and authentication 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.
FTA_TSE.1	Support access limit by IP-based ACL. A series of whitelists and blacklists are set to filter IP addresses and data on ports. Unauthorized IP addresses and communication ports cannot access the system. Support authenticated user logins using the TLS mode.
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 60 minutes.

6.2 Authorization

The TOE enforces an access control by supporting following functions in Table 6-2:

- 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 6-2.
- 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 6-2 Correspondence of user groups and command levels

User group	Command Level
Monitor	Monitor
Operate	Monitor Operate
Maintenance	Monitor Operate Maintenance
Administrator	Monitor Operate 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 level and cannot increase the user level attribute beyond their own user level. Command levels cannot be changed by users.

(FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UID.2, 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)

Table 6-3 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 1-2. In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user level and cannot increase the user level attribute beyond their own user level. Command levels cannot be changed by users.
FDP_ACF.1, FIA_ATD.1, FIA_UID.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 1-2. 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:
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 error message is displayed and the attempt is audited. The authority of each user group is specified in table 1-2. 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:
FMT_MSA.1/ACFATD FMT_MSA.1/IFF FMT_MSA.3/ACFATD FMT_MSA.3/IFF 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 1-2. 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:
FMT_SMR.1	There are four hierarchical user groups (from low to high): monitor, operator, maintenance, and administrator.

6.3 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 user name (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.
- Support for user individual attributes including the user ID ensures that each user is unique in the system and that user-related audit events can be attributed to a user.

(FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3)

Table 6-4 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 user name. 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 user name.
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.

6.4 Communication Security

The TOE provides communication security by implementing trusted channels between the EMS and the TOE 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. 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. 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 following TLS ciphers are supported by the TOE:

TLS1.2:

- 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_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

TLS1.3:

- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC8439
- TLS_AES_256_GCM_SHA384 as defined in RFC8446
- TLS_AES_128_CCM_8_SHA256 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 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 diffie-hellman-group 14-sha1
- The public key algorithm of the SSH transport implementation is ssh-rsa.
- For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported.
- For data integrity protection HMAC-SHA256, 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)

Table 6-5 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 EMS and the TOE 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. 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. The following TLS ciphers are supported by the TOE: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 as defined in RFC8439 TLS_AES_256_GCM_SHA384 as defined in RFC8446 TLS_AES_128_CCM_8_SHA256 as defined in RFC8446 TLS_AES_128_GCM_SHA256 as defined in RFC8446 TLS_AES_128_CCM_SHA256 as defined in RFC8446
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 diffie-hellman-group 14-sha1 The public key algorithm of the SSH transport implementation is ssh-rsa.

	For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported. For data integrity protection HMAC-SHA256, HAMC-SHA512 are supported.

6.5 Management Traffic Flow Control

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

IP-based ACL is provided to filter traffic flow on management interface by matching all or some attributes, including the source IP address, destination IP address, IP protocol number, TCP/UDP source port, and TCP/UDP destination port, 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 6-6 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, destination IP address, IP protocol number, TCP/UDP source port, and TCP/UDP destination port, and then performs actions such as permit, or discard accordingly. The TOE enforces application of ACLs to IP packets from the management network.
FMT_SMF.1	The TOE supports creation, modification and deletion of ACLs.
FTA_TSE.1	IP-based ACL is provided to filter traffic flow on management interface by matching all or some attributes, including the source IP address, destination IP address, IP protocol number, TCP/UDP source port, and TCP/UDP destination port, and then performs actions such as permit, or discard accordingly, thus being able to deny session establishment based on those criteria.

6.6 Security Management

The TOE allows management of the equipment network by different users. The TOE can be configured to grant each user the access right to the equipment network resources that are required for user operations. The functions mainly include:

- User management, including the user name and passwords.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling of TLS for the communication between EMS and the TOE.
- Definition of IP addresses and address ranges for clients and server that are allowed to connect to the TOE.
- Set-up and modification of ACL policy.

All of these management options are generally available via the EMS.

Detailed functions mainly include:

- Support remote TOE management using TLS.
- Support automatic account logout when no operation is performed on the user session within a specified interval.
- Support the maximum attempts for authentication failures within certain period of time.
- Support ACL filtering based on IP protocol number, source and/or destination IP address, or source and/or destination port.
- Support the address configuration of the RADIUS server.
- Support the address configuration of the Syslog server.
- Support the address configuration of the NTP server.
- Support the address configuration of the SFTP server.
- Support setting the time information on the TOE.

The TOE management can use two kinds of sessions for administrative activities based on different protocols:

- QX is a proprietary interface between EMS and TOE. EMS uses QX commands to implement OAM (Operation Administration and Maintenance) function on TOE. The TOE provides abundant QX commands to allow the users to manage the TOE.
- MML commands are used mainly for local maintenance tasks like fault location and software upgrades. For this evaluation, MML commands are used to up- and download files via the TOE’s SFTP client.

Note that users cannot have QX and MML sessions at the same time.

(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)

Table 6-7 SFR to TSF mapping

SFR	TSF
FMT_MOF.1, FMT_MSA.1/ACTATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD, FMT_SMF.1, FMT_SMR.1	The TOE allows management of the telecommunications network by different users. The TOE can be configured to grant each user the access right to the telecommunications network resources that are required for user operations. The functions mainly include: User management, including the user name and passwords. Access control management, including the association of users and corresponding privileged functionalities. Enabling/disabling of TLS for the communication between EMS and the TOE.

	Definition of IP addresses and address ranges for clients and server that are allowed to connect to the TOE. Set-up and modification of ACL policy. All of these management options are generally available via the EMS. Detailed functions mainly include: Support remote TOE management using TLS. Support SFTP enable and disable. Support automatic account logout when no operation is performed on the user session within a specified interval. Support the maximum attempts for authentication failures within certain period of time. Support configuration of the RADIUS server. Support configuration of the Syslog server. Support configuration of the NTP server. Support configuration of the SFTP server. Support setting the time information on the TOE.
FMT_MSA.3/IFF	The ACL filtering mechanism is enforcing the Management Network Filtering SFP. By default, no ACL rules are configured therefore all traffic will be allowed to pass. Administrators 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, Administrators can change the default behavior where all traffic is allowed to pass.

A Abbreviations, Terminology and References

A.1 Abbreviations

CC	Common Criteria
DCN	Data Communications Network (the management network)
EMS	Element Management System
LCT	Local Craft Terminal
LMT	Local Maintenance Terminal
MSTP	Multi-Service Transmission Platform
OSN	Optical Switch Node
OTN	Optical Transport Network
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RMT	Remote Maintenance Terminal
RSA	Rivest Shamir Adleman
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
WDM	Wavelength Division Multiplexing

AGD_OPE	Operational User Guidance
AGD_PRE	Preparative Procedures
ADV_C&R	Configuration and Reference

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

[CC]	Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, April 2017
[AIS20]	Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, Version 2.0, 2 December 1999
[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 SP800-38D]	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 SP800-56B]	NIST Special Publication 800-56B Rev. 2 – Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, July 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 1321] The MD5 Message-Digest Algorithm, R. Rivest, April 1992

[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 4346] RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1, April 2006

[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 5289] TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

[RFC 8439] ChaCha20 and Poly1305 for IETF Protocols, June 2018

[RFC 6655] AES-500CCM Cipher Suites for Transport Layer Security (TLS), July 2012

[RFC 5116] An Interface and Algorithms for Authenticated Encryption, January 2008

[RFC 8018] PKCS #5: Password-Based Cryptography Specification Verion 2.1, B. Kaliski, 2017-01-01

[RFC 8446] RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3, August 2018