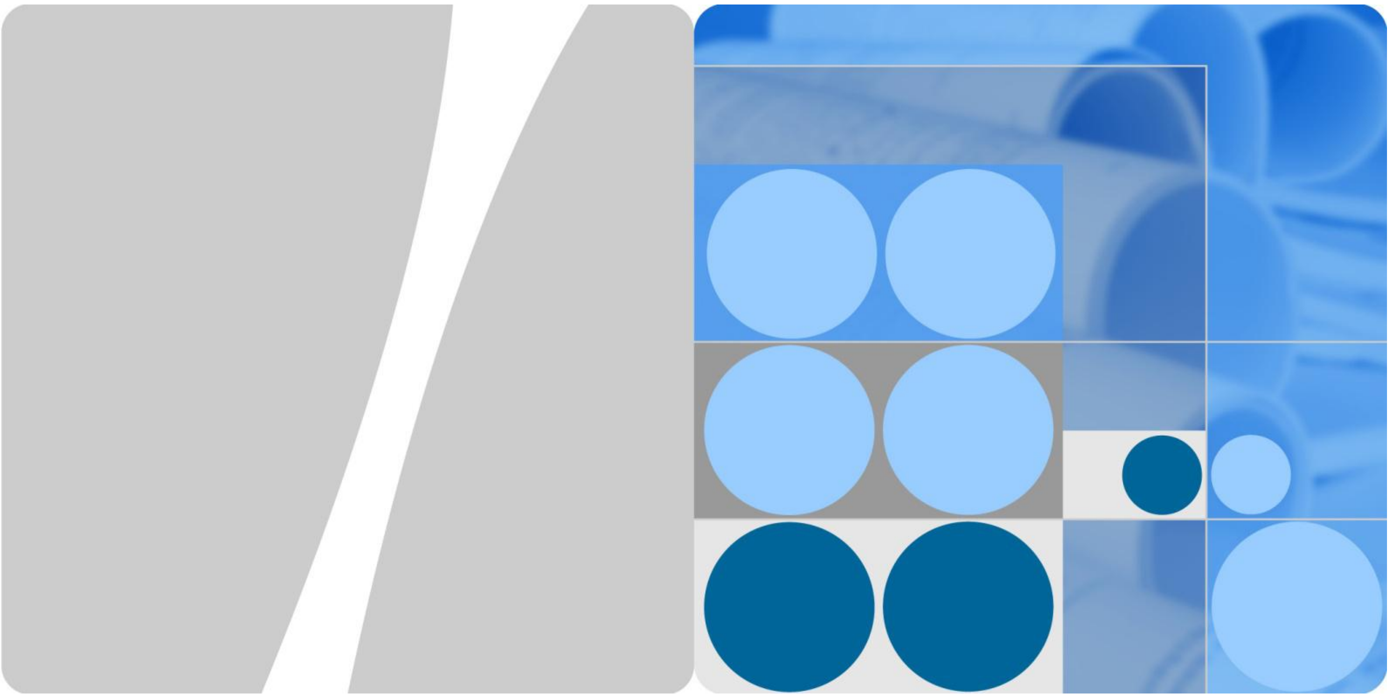


CC Huawei OptiX PTN Series Products V100R009 Security Target

Version **V0.5**

Date **2019-04-11**

HUAWEI TECHNOLOGIES CO., LTD.

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

Contents

1 Introduction

This Security Target is for the evaluation of Huawei OptiX PTN Series Products.

1.1 ST Reference

Title CC Huawei OptiX PTN Series Products V100R009 Security Target

Version V0.5

Author Huawei Technologies Co., Ltd.

Date of publication 2019-04-11

1.2 TOE Reference

TOE Name Huawei OptiX PTN Series Products

TOE Developer Huawei Technologies Co., Ltd.

TOE Version

There are seven types of evaluated platforms of the PTN Series products and two types of evaluated software (V100R009C10SPC100 & V100R009C00SPC200). Both, platforms and software running on them, are considered TOE and the correspondence between the platforms and the software version running on them is the following:

Table 1–1 Types of chassis and software used in OptiX PTN Series products

Evaluated platform identifier	Software version
Optix PTN 7900-32	V100R009C10SPC100
Optix PTN 7900-24	V100R009C10SPC100
Optix PTN 7900-12	V100R009C10SPC100
Optix PTN 905E	V100R009C00SPC200
Optix PTN 910E-F	V100R009C10SPC100
Optix PTN 970	V100R009C10SPC100
Optix PTN 990	V100R009C10SPC100

In general, PTN7900-32, PTN7900-24 and PTN7900-12 are PTN7900 device form.

1.3 Target of Evaluation (TOE) Overview

1.3.1 TOE Type

The TOE is a Network Element composed of a hardware platform and a software running within the platform as a whole system. The underlying operating system contained in the evaluated platforms (RTOS) is not part of the TOE. Based on the powerful versatile routing platform (VRP), the OptiX PTN provides strong switching capabilities, dense ports, and high reliability.

1.3.2 TOE usage & Major Security Features

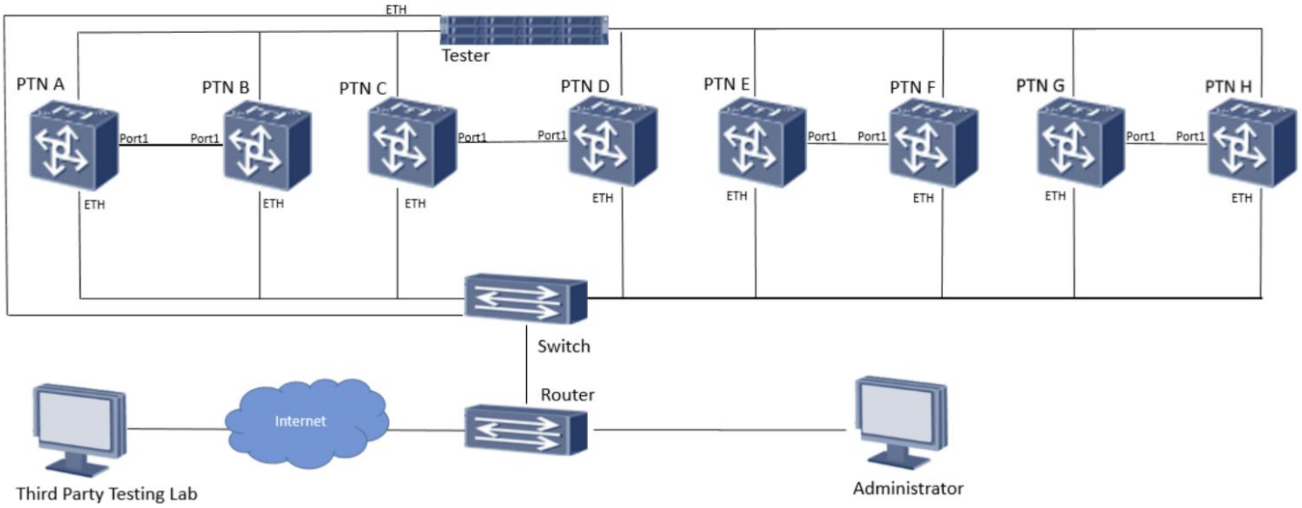
OptiX PTN is located in the core layer, aggregation layer and access layer of the metro transport network. It sets up the network of various types of services such as mobile communication and group customers. OptiX PTN series support mainly Layer 3 forwarding .

The major security features include: Authentication, Access Control, ACL, Auditing, Communication Security, Flow Control Policy, Security Management, Cryptographic functions.

1.3.3 Non TOE Hardware/Software/Firmware

The Figure 1-2 shows a sample TOE deployment, and the logical interconnections to/from TOE components.

Figure 1-2 TOE Deployment Diagram



The Table 1-2 shows that TOE supports hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 1-2 IT Environment Components

Component	Required	Usage/purpose Description for TOE performance
Administrator	Yes	The PC (Personal Computer) includes any IT Environment Management Software installed that is used by the TOE administrator for administration of the TOE.
Internet	Yes	The public network.
Third Party Testing Lab	Yes	Stand for third party labs or personal engaged in the testing and evaluation of the TOE.
Router	Yes	A device that connects internet and local network environment and automatically distribute data through the best possible route according to the condition of the trusted channels.
Switch	Yes	A device that connects TOE and other components of the operational environment according to user's need.
Tester	Yes	A testing platform installed with software like Tesgine or Spirent Testcenter. It is deployed for the test of SSH protocol and to capture ingoing and outgoing packets between devices ports.

The underlying operating system (RTOS) contained in each evaluated platform is not part of the TOE but it is needed to run the evaluated software packages.

1.3.4 Excluded Functionality of the TOE

The functionality Table 1-3 included in the following is excluded from the evaluation.

Table 1–3 Excluded Functionality

Excluded Functionality	Excluded Rationale
BGP, ISIS, OSPF	BGP ISIS, OSPF will be disabled in the evaluated configuration
RSVP	RSVP will be disabled in the evaluated configuration
SNMP	SNMP will be disabled in the evaluated configuration
TOE management through Netconf interface (port 830)	Netconf interface will be disabled in the evaluated configuration
TOE management through DCN interface (ports 1400 and 5432)	DCN interface will be disabled in the evaluated configuration.

1.4 TOE Description

1.4.1 Physical Scope

This section will introduce the OptiX PTN V100R009 from a physical architectural view and a physical scope view.

1.4.1.1 Physical Boundary

Huawei relies on 3rd party shipping companies to deliver products from the production facility to users. Huawei has a contractual agreement on Logistics Security that they have signed with all of these companies. Staff of the production facility shall notify the user of the shipping company that will ship the TOE in advance.

1.4.1.1.1 Physical Architecture of OptiX PTN 7900-32

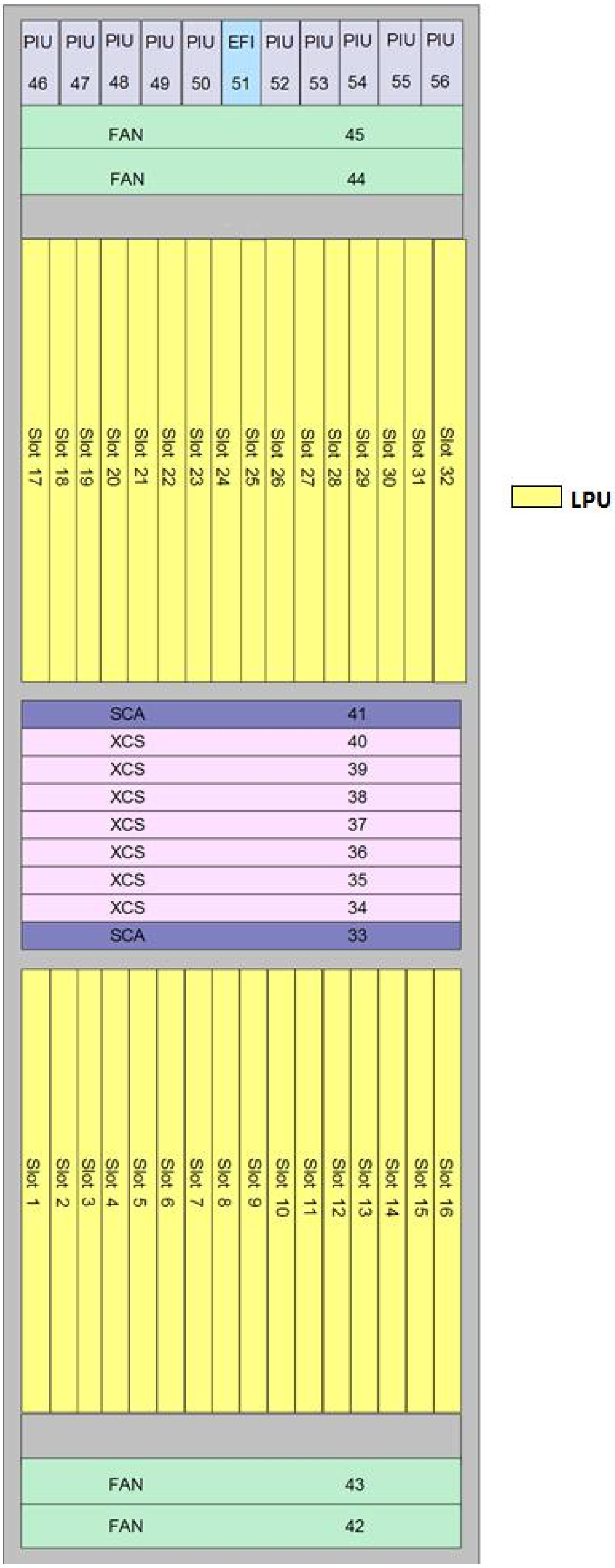
An OptiX PTN 7900-32 consists of the following systems:

- Power distribution system
- Heat dissipation system
- Functional host system

The functional host system of SCAs(a type of main control board), LPUs (Line Process Unit, interface board), XCSs (Cross-connect and Synchronous Timing Board) are depicted in Figure 1-3. The functional host system manages and controls the other systems, and provides control and data channels.

The SCA is responsible for the completion of system control functions. The XCS is responsible for the business scheduling. And the interface board (LPU) helps the XCS to complete the business processing and forwarding.

Figure 1-3 The functional host system of OptiX PTN 7900-32



1.4.1.1.2 Physical Architecture of OptiX PTN 7900-24

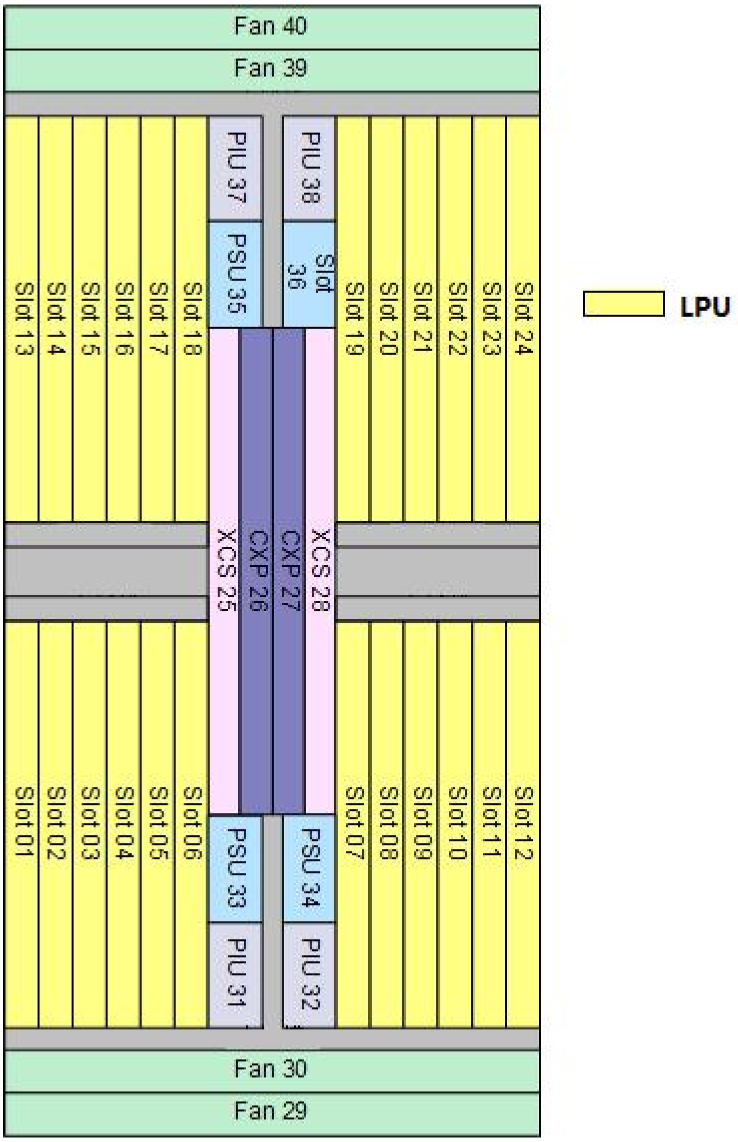
An OptiX PTN 7900-24 consists of the following systems:

- Power distribution system
- Heat dissipation system
- Functional host system

The functional host system of CXPs (a type of main control board), LPUs, XCSs are depicted in Figure 1-3. The functional host system manages and controls the other systems, and provides control and data channels.

The main control board (CXP) is responsible for the completion of system control functions. The XCS is responsible for the business scheduling. And the LPU helps XCS to complete the business processing and forwarding.

Figure 1–4 The functional host system of OptiX PTN 7900-24



1.4.1.1.3 Physical Architecture of OptiX PTN 7900-12

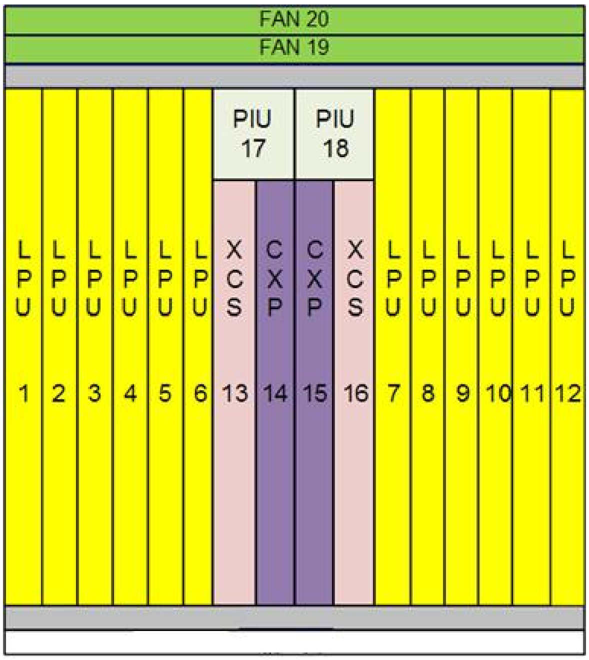
An OptiX PTN 7900-12 consists of the following systems:

- Power distribution system
- Heat dissipation system
- Functional host system

The functional host system of CXPs, LPUs, XCSs depicted in Figure 1-4. The functional host system manages and controls the other systems, and provides control and data channels.

The main control board (CXP) is responsible for the completion of system control functions. The XCS is responsible for the business scheduling. And the LPU helps XCS to complete the business processing and forwarding.

Figure 1-5 The functional host system of OptiX PTN 7900-12



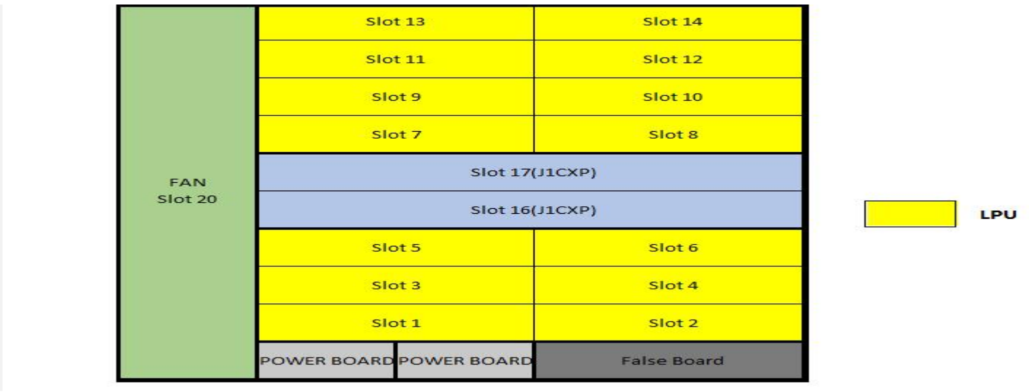
1.4.1.1.4 Physical Architecture of OptiX PTN 990

An OptiX PTN 990 consists of the following systems:

- Power distribution system
- Heat dissipation system
- Functional host system

The functional host system consists of MPUs (a type of main control board) and LPUs. The LPUs can be divided into Ethernet interface board, E1 interface board and SDH interface board.

Figure 1-6 The functional host system of OptiX PTN 990



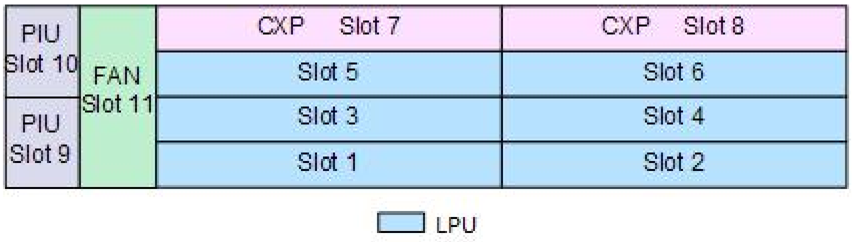
1.4.1.1.5 Physical Architecture of OptiX PTN 970

An OptiX PTN 970 consists of the following systems:

- Power distribution system
- Heat dissipation system
- Functional host system

The functional host system consists of MPUs and LPUs. The LPUs can be divided into Ethernet interface board, E1 interface board and SDH interface board.

Figure 1-7 The functional host system of OptiX PTN 970



1.4.1.1.6 Physical Architecture of OptiX PTN 910E-F

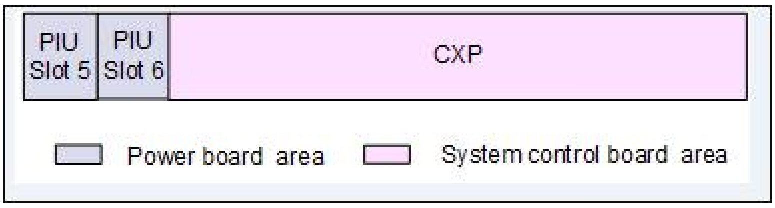
A PTN 910E-F consists of the following systems :

- Power distribution system
- Heat dissipation system

- Functional host system

The functional host system of a PTN 910E-F consists of a MPU. The functional host system manages and controls the other systems, and provides control and data channels.

Figure 1-8 The functional host system of OptiX PTN 910E-F



1.4.1.1.7 Physical Architecture of OptiX PTN 905E

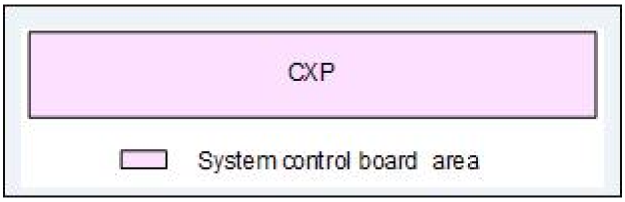
A PTN 905 consists of the following systems :

- Power distribution system
- Heat dissipation system
- Functional host system

All PTN 950E's systems are in the integrated cabinet. The functional host system is the target of this evaluation and the following introductions will focus on the functional host system only. The Network management system, power distribution system and heat dissipation system are not within the scope of this evaluation.

The functional host system of a PTN 905E consists of a MPU. The functional host system manages and controls the other systems, and provides control and data channels.

Figure 1-9 The functional host system of OptiX PTN 905E



1.4.1.2 Physical scope list

This section will define the physical scope of the OptiX PTN V100R009 to be evaluated. The lists of evaluated documents and software packages are:

Document name	Version:	SHA256 Hash checksum
CC OptiX PTN Series Product V100R009 Preparative Procedures for Production	Version: 0.4	5d887f0d98ad52503b5237945cd017de31f01e2d929902d23f127e82311369af
CC OptiX PTN Series Product V100R009 Operational User Guide	Version: 0.4	9a95de8927b3cad087549c65200bb2e638d9a684e5574c0ae42a1bf5aef3beda

Preparative procedures and Operational Guidance can be downloaded from official website via the authorized customer account. The user shall follow these documents in order to bring the TOE to the evaluated configuration with the following protocols disabled: BGP, ISIS, OSPF, RSVP, SNMP, Netconf and DCN.

Document name	Version:	SHA256 Hash checksum
OptiX PTN 905E V100R009C00 Command Reference 02.chm	0.2	f214644e46fa089fa8a03447d2e6017bd81d49d499e5eea7584ef75a3cc2b5b1
OptiX PTN 910E-F V100R009C10 Command Reference 01.chm	0.1	f9dc59b00ed15b70dbd93b886c3e3f817d0906b90cac7aa11561a1456a87cf91
OptiX PTN 990&970 V100R009C10 Command Reference 01.chm	0.1	22a6504998a79b7276a545141be

		38926e13235591b67a98a707c4ebd7fa86a54
OptiX PTN 7900 V100R009C10 Command Reference 01.chm	0.1	b8bab3f6c1f02e2239a517f044414356d49444e0eb3d382c94a1938f7f398cc2
OptiX PTN 905E V100R009C00 Product Documentation 02.zip	0.2	f35bc3474fb69477e949d2c607bbe838b1074e2732fed560a84d8da9e52f511d
OptiX PTN 910E-F V100R009C10 Product Documentation 03.zip	0.3	159398a5841f0eb1e3614502ac290286ab16f4d9324de596022e6bde005cf1e0
OptiX PTN 970 V100R009C10 Product Documentation 03.zip	0.3	6d33c18959bc87ff4e176b19141c52f10ddd54dd92093dbd068706feb19ce669
OptiX PTN 990 V100R009C10 Product Documentation 03.zip	0.3	018e14f7c8ee4f31be9428a507ff941b86347fd62d7b5f5a3f3dd96b9572c7ac
OptiX PTN 7900-12 V100R009C10 Product Documentation 03.zip	0.3	21d70145b8ece67a5968f046c3db5ee82be49f08e8fd7136

		083aabbbbd823dcc
OptiX PTN 7900-24 V100R009C10 Product Documentation 03.zip	0.3	50c2130750d637315734bd7967d2f6758787800fbf3263f9b8d8b159d4f220222
OptiX PTN 7900-32 V100R009C10 Product Documentation 03.zip	0.3	8861ddb9a7724c193b6f912e57d2d0cff7de499e1d1db69f3e2b79160f37e337

Product documentation and command reference can be downloaded from official website via the authorized customer account.

Package name	Software	Platform ID	Software version
OptiX PTN 905E V100R009C00SPC200.zip.asc	PTN90XV100R009C00SPC200.cc	905E	V100R009C00SPC200
OptiX PTN 910E-F V100R009C10SPC100.zip.asc	PTN910E-FV100R009C10SPC100.cc	910F	V100R009C10SPC100
OptiX PTN 970 V100R009C10SPC100.zip.asc	PTN970V100R009C10SPC100.cc	970	V100R009C10SPC100
OptiX PTN 990 V100R009C10SPC100.zip.asc	PTN990V100R009C10SPC100.cc	990	V100R009C10SPC100
OptiX PTN 7900-12 V100R009C10SPC100.zip.asc	PTN7900V100R009C10SPC100.cc	7900-12	V100R009C10SPC100

OptiX PTN 7900-24 V100R009C10SPC100 .zip.asc	PTN7900V100R009C10SPC100.cc	7900-24	V100R009C10SPC100
OptiX PTN 7900-32 V100R009C10SPC100 .zip.asc	PTN7900V100R009C10SPC100.cc	7900-32	V100R009C10SPC100

Packages containing the TOE software can be downloaded from official website via the authorized customer account.

The TOE provides several models including single-chassis systems and cluster systems. These models differ in their modularity and throughput by deploying different LPUs or different number of chassis, but they offer exchangeable forwarding unit modules, switch fabrics, and use the same version of software.

There are 7 types of chassis of an PTN chassis as shown in Table 1-1. And there some LPUs of PTN are shown in Table 1-5, Table 1-6 , Table 1-7.

The following boards will be covered during this evaluation :

Table 1–4 List of boards

Product Name	Board Name for Order	Description
OptiX PTN 7900-32	TPA1SCA	Master and communication processing unit
	TPA1XCS	Switched network unit
	TPA2XCS	Switched network unit
OptiX PTN 7900-24	TPB1CXP	Master crossed multiprotocol processing board
	TPB2CXP	Master crossed multiprotocol processing board
	TPB3CXP	Master crossed multiprotocol processing board
	TPB1XCS	Switched network unit
	TPB2XCS	Switched network unit
	TPB3XCS	Switched network unit
OptiX PTN 7900-12	TPC1CXP	Master crossed multiprotocol processing board

	TPC2CXP	Master crossed multiprotocol processing board
	TPC1XCS	Switched network unit
	TPC2XCS	Switched network unit
OptiX PTN 990	TPJ1CXP	Main Processing Unit
	TPJ2CXP	Main Processing Unit
OptiX PTN 970	TPK1CXPA	Main Processing Unit
OptiX PTN 910E-F	TPP1CXP	Main Processing Unit
OptiX PTN 905E	TPM1CXPL	Main Processing Unit

Table 1-5 LPUs and the corresponding FPICs for OptiX PTN 7900

Order Name	Name
TPA1EHD1	1-way 200GE Ethernet processing board
TPA1EH2	2-way 100GE Ethernet processing board
TPA2EH2	2-way 100GE Ethernet processing board
TPA1EH1	1-way 100GE Ethernet processing board
TPA2EH1	1-way 100GE Ethernet processing board
TPA3EH1	1-way 100GE Ethernet processing board
TPA1EXL1	1-way 40GE Ethernet processing board
TPA1EXL2	2-way 40GE Ethernet processing board
TPA2EXL2	2-way 40GE Ethernet processing board
TPA1EX4	4-way 10GE Ethernet processing board
TPA1EX8	8-way 10GE Ethernet processing board
TPA1EX8S	8-way 10GE Ethernet processing board
TPA1EX12	12-way 10GE Ethernet processing board
TPA1EX16S	16-way 10GE Ethernet processing board
TPA1EG16	16-way GE / FE adaptive Ethernet processing board
TPA1EG24	24-way GE / FE adaptive Ethernet processing board
TPA2EG24	24-way GE / FE adaptive Ethernet processing board

Order Name	Name
TPA1MPA	Multi-interface GE / STM-1 / E1 processing board
TPA1CO1	8-way channelized STM-1 processing board
TPA1CH1	16-way channelized STM-1 processing board
TPA1CQ4	4-way channelized STM-4 processing board
TPA1MQ1	63-way E1 processing board
TPA3EH2	2-way 100G Ethernet processing board
TPA1EV4	4-way 50G Ethernet processing board
TPA1EH4	4-way 100G Ethernet processing board
TPA1EX20A	20-way 10G Ethernet color light processing board
TA124:A150PA1EH2A	2-way 100G Ethernet color light processing board

Table 1-6 LPUs and the corresponding FPICs for OptiX PTN 990

Order Name	Name
TPJ1EX2S	2-way 10GE Ethernet interface board
TPJ1EM8F	8-way GE / FE optical interface board
TPJ1EM8T	8-way GE / FE electrical interface board
TPJ1ML1A/TPJ1ML1B	16-way E1 interface board
TPJ1MD1A/TPJ1MD1B	32-way E1 interface board
TPJ1SQ1	4-way STM-1 optical interface board
TPJ1EXL1	1 way 40GE Ethernet interface board
TPJ1EX1S	1 way 10GE Ethernet interface board
TPJ1EH1	1 way 100GE optical interface board
TPJ2EH1	1 way 100GE optical interface board
TPJ1EX4S	4-way 10GE optical interface board (SFP +)
TPJ1EV2	2-way 50GE optical interface board

Table 1–7 LPUs and the corresponding FPICs for OptiX PTN 970

Order Name	Name
TPK1EXL1	1 way 40GE Optical interface board
TPK1EX1S	1 way 10GE Optical interface board
TPK1EX2S	2-way 10GE Optical interface board
TPK1EM8F	8-way GE / FE optical interface board
TPK1EM8T	8-way GE / FE electrical interface board
TND1EG2	2-way GE optical interface board
TND2EG2	2-way GE optical interface board
TND1EF8F	8-way FE optical interface board
TND1EF8T	8-way FE electrical interface board
TPK1ML1A	16-way E1 interface board
TPK1ML1B	16-way E1 interface board
TND2ML1A	16-way E1 interface board
TND2ML1B	16-way E1 interface board
TPK1MD1A	32-way E1 interface board
TPK1MD1B	32-way E1 interface board
TPK1SQ1	4-way circuit simulation interface board

1.4.2 Logical Scope

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below:

1. Authentication
2. Access Control
3. ACL
4. Auditing
5. Communication Security
6. Security functionality management
7. Cryptographic functions

1.4.2.1 Authentications

The TOE can authenticate administrative users by user name and password by RSA/DSA. VRP provides a local authentication scheme for this. Authentication is always enforced for virtual terminal sessions via SSH. Authentication is always required for access through TOE's ETH interface. The TOE will establish the session after successful authentication, and terminate the session after the users log out. When the number of unsuccessful authentication attempts has been surpassed, the TOE terminates the session of the user and lock the user for 5 minutes.

1.4.2.2 Access Control

1.4.2.2.1 User Group

The TOE controls access by user groups. The user's type is determined by one of the 4 hierarchical user groups it is assigned to.

User groups are predetermined by the product itself as displayed in Table 1-8. New Users can be created and assigned to a user group which has its own predetermined command set (Default level - Every).

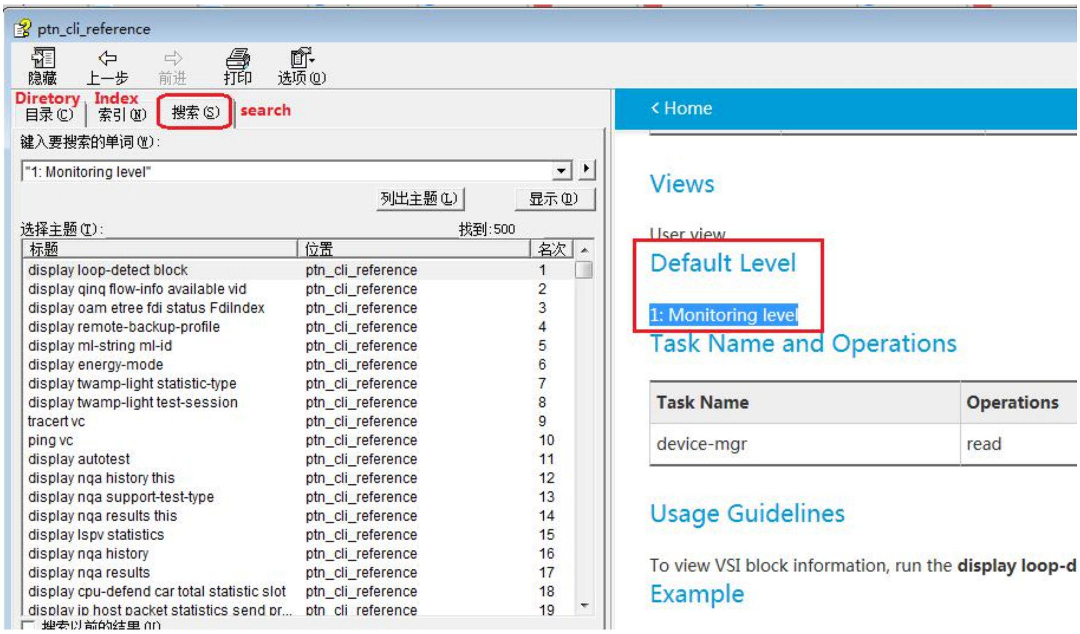
Table 1-8 User Groups

Group ID	Group name	Description
4	Every	Login/logout, and password modification, query on commands of some services. Default level.
3	Operator	Partial system-level queries and partial performance queries and configurations. All Visit level and Monitoring level commands can be executed
2	Maintainer	Partial system-level and security queries and most of configuration and communication settings. All Visit level, Monitoring and Configuration level commands can be executed
1	Administrator	All queries and configurations, security settings (log management included) Administrator level, all commands can be executed

1.4.2.2.2 Command Levels

In the command manual, each command has a default level, only users of the current level or a higher level can perform this command. Command level of a command can be found in the command manual under "Default

Level", e.g. keyword "1: Monitoring level" (with "") can be used to gather all the commands with the default level of "monitoring", so is "0: Visit", "2: Configuration" and "3: Management".



标题	位置	名次
display loop-detect block	ptn_cli_reference	1
display qinq flow-info available vid	ptn_cli_reference	2
display oam etree fdi status FdiIndex	ptn_cli_reference	3
display remote-backup-profile	ptn_cli_reference	4
display ml-string ml-id	ptn_cli_reference	5
display energy-mode	ptn_cli_reference	6
display twamp-light statistic-type	ptn_cli_reference	7
display twamp-light test-session	ptn_cli_reference	8
tracert vc	ptn_cli_reference	9
ping vc	ptn_cli_reference	10
display autotest	ptn_cli_reference	11
display nqa history this	ptn_cli_reference	12
display nqa support-test-type	ptn_cli_reference	13
display nqa results this	ptn_cli_reference	14
display lspv statistics	ptn_cli_reference	15
display nqa history	ptn_cli_reference	16
display nqa results	ptn_cli_reference	17
display cpu-defend car total statistic slot	ptn_cli_reference	18
display ip host packet statistics send pr...	ptn_cli_reference	19

Views

User view

Default Level

1: Monitoring level

Task Name and Operations

Task Name	Operations
device-mgr	read

Usage Guidelines

To view VSI block information, run the **display loop-d**

Example

Table 1-9 Command Level.

Level Id	Level name	Description
0	Visit	Login/logout, and password modification, query on commands of some services. Default level.
1	Monitoring	Partial system-level queries and partial performance queries and configurations. All Visit level and Monitoring level commands can be executed
2	Configuration	Partial system-level and security queries and most of configuration and communication settings. All Visit level, Monitoring and Configuration level commands can be executed
3	Management	All queries and configurations, security settings (log management included). Administrator level, all commands can be executed

1.4.2.2.3 Mapping between User Group and Command Levels

Users once created should be assigned to a specific user group to gain access to its corresponding command set. Each Command level is matched to a unique Group ID as following diagram shows.

Group ID	Group name	Level Id	Level name
4	Every	0	Visit
3	Operator	1	Monitoring
2	Maintainer	2	Configuration
1	Administrator	3	Management

The groups “Every, Operator, Maintainer and Administrator” are named as “every, oper, main and admin” when they are used in the TOE.

1.4.2.3 ACL

VRP offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces on LPU. Information flow that is processed with ACL and to be forwarded to other network interfaces is within the scope of the evaluated configuration.

The administrator can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE through interfaces on LPU by matching information contained in the headers of IP packets against ACL rules specified. Source IP address, destination IP address, IP protocol number, source port number of TCP/UDP protocol, destination port number of TCP/UDP protocol, TCP flag of TCP protocol etc, can be used for ACL rule configuration.

1.4.2.4 Auditing

VRP generates audit records for security-relevant management actions and stores the audit records in CF card inserted into TOE.

- By default all correctly input and executed commands along with a timestamp when they are executed are logged.
- Attempts to access is logged, no matter whether it is succeeded access or failed access, along with user id, source IP address, timestamp etc.
- Review functionality is provided via the command line interface, which allows administrators to inspect the audit log.
- The oldest files will be deleted when the audit trail exceeds the size of the storage device.

1.4.2.5 Communication Security

The TOE provides communication security by implementing SSH protocol. SSH2 (SSH2.0) is implemented, and SSH2 is recommended for most cases by providing more secure and effectiveness in terms of functionality and performance.

To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH provides:

- authentication by password and by RSA/DSA;
- AES encryption algorithms;
- verify user data by sha2 algorithms
- Secure cryptographic key exchange.

Besides default TCP port 22, manually specifying a listening port is also implemented since it can effectively reduce attack.

1.4.2.6 Security functionality management

Security functionality management includes 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.

More functionalities include:

- authentication, authorization, encryption policy
- ACL policy
- user management
- port security
- maximum number of user logins
- configure the interval for user inactivity after that an established session is terminated

1.4.2.7 Cryptographic functions

Cryptographic functions are required by security features as dependencies, where:

AES is used as default encryption algorithm for SSH;

RSA and DSA are used in user authentication when user tries to authenticate.

SHA-2 is used as verification algorithm for packets of SSH protocols.

DH is used as an exchange algorithm of encryption keys for data transmission of SSH protocols packets.

All passwords are case sensitive, and the password length will be check when the password be used.

2 CC Conformance Claim

This ST is CC Part 2 conformant and CC Part 3 conformant [CC]. There are no extended components defined for CC Part 3 and CC Part 2. The CC version used is 3.1R5.

No conformance to a Protection Profile is claimed.

This ST is conforming to assurance package EAL3 without augmentations.

3 TOE Security problem definition

3.1 Threats

The assumed security threats are listed below.

The availability, confidentiality and integrity **information assets** to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, audit records, etc.) and other information that the TOE facilitates access to (such as system software, patches and network traffic routed by the TOE) are all considered part of information assets.

The threats to the TOE are identified and detailed in Table 3-1.

Table 3–1 List of identified threats

Threat Name	Threat Definition
T.UnwantedNetworkTraffic	Any network user that sends unwanted/unexpected L3 network traffic to/through the TOE will reach resources on the network that it is not allowed to reach.
T.UnauthenticatedAccess	A subject that is not an authenticated user of the TOE gains access to the TOE and modifies TOE configuration data without permission.
T.UnauthorizedAccess	A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for. By that he could modify TOE configuration data without permission. This threat also includes data leakage to non-intended person or device

Threat Name	Threat Definition
T.Eavesdrop	An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and PC.

3.2 Assumptions

3.2.1 Environment of use of the TOE

3.2.1.1 Physical

A.PhysicalProtection It is assumed that the TOE (including any console attached, access of CF card) is protected against unauthorized physical access. The TOE is assumed not to contain any residual information that could be used for an attack when it is removed from the physically protected environment (e.g. for repair by a third party or at the end of life when the device is disposed).

3.2.1.2 Network Elements

A.NetworkElements The environment is supposed to provide 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 devices are:

- Peer router(s) for the exchange of dynamic routing information;
- A remote entities (PCs) used for administration of the TOE.

3.2.1.3 Network Segregation

A.NetworkSegregation It is assumed that the ETH interface on MPU in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks where the interfaces on LPU in the TOE are accessible.

3.2.1.4 Personnel Assumptions

A.Noevil The authorized users except the users “every” with level id 0 will be trustworthy, competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation. In this way operators, maintainers and administrators will not try to modify the date of the device.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Forwarding** The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds to a configured route for the destination IP address of the packet (L3 routing). The TOE shall provide Access Control List (ACL) functionality that can be configured to drop unwanted network traffic.
- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and PC from the operational environment.
- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to administrators and users in order to restrict the functionality that is available to them.
- **O.Authentication** The TOE must authenticate users of its user access.
- **O.Audit** The TOE shall provide functionality to generate and protect audit records for security-relevant actions.

4.2 Objectives for the Operational Environment

- **OE.NetworkElements** The operational environment shall provide 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. For example, other routers for the exchange of routing information, PCs used for TOE administration.
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console, and CF card inserted in the MPU) shall be protected against unauthorized physical access. Whenever the TOE is

removed from the physically protected environment, it shall not contain any residual information that could be used for an attack.

- **OE.NetworkSegregation** The operational environment shall provide segregation by deploying the Ethernet interface on MPU in TOE into a local sub-network, compared to the interfaces on LPU in TOE serving the application (or public) network.
- **OE.Person** Personnel working as authorized administrators (authorized users except the users “every” with level id 0) shall be carefully selected for trustworthiness and trained for proper operation of the TOE.

4.3 Security Objectives Rationale

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

Table 4–1 Mapping Objectives to Threats

Threat	Rationale for security objectives to remove threats
T.UnwantedTraffic	This threat is countered by O.Forwarding, filtering the traffic intended to be forwarding according with an ACL.
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSHv2 for communication between users (including PC and laptop). (O.Communication).

The following table provides a mapping of the objectives for the operational environment to assumptions, threats and policies, showing that each objective is covered by at least one assumption, threat or policy.

Table 4-2 Mapping Objectives for the Environment to Assumptions

Environmental Objective	Assumption
A.NetworkElements	The assumption that the external environment provides securely and correctly working network devices such as peer device for routing information exchange, and management terminals for TOE control and management is addressed in OE.NetworkElements.
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access and that the TOE does not contain residual information that could be used for an attack whenever the TOE is removed from the physically protected environment is expressed by a corresponding requirement in OE.Physical.
A.NetworkSegregation	The assumption that the TOE managed by ETH interface deployed in the MPU is not accessible via the application (or public) networks hosted by the networking device is addressed by requiring just this in OE.NetworkSegregation.
A.NoEvil	The assumption that the authorized users of the TOE (except the users “every” with level id 0) are not careless, willfully negligent, or hostile is addressed in OE.Person.

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 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.
- /CONTEXT: indicates the context of the iteration

6.2 TOE Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

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

1. Start-up and shutdown of the audit functions;
2. All auditable events for the ***[not specified]*** level of audit; and
3. **[The following auditable events:**

   i. user activity

      1. login, logout

      2. operation requests

   ii. User management

      1. add, delete, modify

2. password change

3. operation authority change

4. online user query

5. session termination

iii. authentication policy modification

iv. system management

1. reset to factory settings

v. log management

log policy modification]

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

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[user IP (if applicable), and CLI command name (if applicable)]**

6.2.1.2 FAU_GEN.2 User identity association

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

6.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[authorized users as defined in FDP_ACF.1]** 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.

6.2.1.4 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]*** unauthorised modifications to the stored audit records in the audit trail.

6.2.1.5 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **[delete the oldest files]** if the audit trail exceeds **[the size of the storage device]**.

6.2.2 Cryptography

6.2.2.1 FCS_COP.1/AES Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[symmetric decryption and encryption]** in accordance with a specified cryptographic algorithm **[AES CTR Mode]** and cryptographic key sizes **[128bits, 256bits]** that meet the following: **[None]**

6.2.2.2 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[asymmetric authentication]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[2048bits]** that meet the following: **[None]**

6.2.2.3 FCS_COP.1/ SHA2 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[cryptographic hashing services]** in accordance with a specified cryptographic algorithm **[SHA2-256]** and cryptographic key sizes **[none]** that meet the following: **[None].**

Application Note: SHA2 is used for hashing within SSH communication. As a hash algorithm it does not require keys to operate.

6.2.2.4 FCS_COP.1/DSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[asymmetric authentication]** in accordance with a specified cryptographic algorithm **[DSA]** and cryptographic key sizes **[2048bits]** that meet the following: **[None]**

6.2.2.5 FCS_CKM.1/AES Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[AES CTR Mode]** and specified cryptographic key sizes **[128 bits, 256 bits]** that meet the following: **[None]**

6.2.2.6 FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA]** and specified cryptographic key sizes **[2048bits]** that meet the following: **[None]**

6.2.2.7 FCS_CKM.1/DSA Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[DSA]** and specified cryptographic key sizes **[2048bits]** that meet the following: **[None]**

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[VRP access control policy]** on

[Subject: users;

Objects: commands provided by TOE;

Operation: Execute]

6.2.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[VRP access control policy]** to objects based on the following:

[Subject security attributes

1. **users and their following security attributes:**

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

Objects security attributes:

2. **commands and their following security attributes:**

- **Command level]**

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

User levels map command levels. A user can only run commands at the same or lower level]

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:

[A user is not allowed to run commands with a user level that is higher than his user level].

6.2.3.3 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce **[ACLs flow policy]** on

[Subjects:

external IT entities that send and receive information through the TOE to one another;

Information:

traffic sent through the TOE from one subject to another;

Operations:

Permit, Deny]

6.2.3.4 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **[ACLs flow policy]** based on the following types of subject and information security attributes **[**

Subject: TOE interface through which traffic goes

Information security attributes:

Packet characteristic: such as Source IP address / Destination IP address / protocol type /Source port / Destination port]

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: **[**

Whenever an incoming management network packet is handled by TCPIP protocol layer 2 (forwarding or accepting) on TOE, the Access Control List (ACL) will be checked.

The ACL rules could either permit or deny forwarding or accepting based on the information security attributes 'source IP address', 'destination IP address', 'protocol type', 'source tcp or udp port number', 'destination tcp or udp port number'. Rules have to contain at least one of the attributes but may contain several attributes.

For every incoming data network packet that is intended to be forwarded or accepted by the TOE the ACL is checked for a rule that matches the attributes of the packet, respectively starting from the first entry in the ACL. The ACL is checked until the first matching rule is found. The network packet is then either passed (forwarded/accepted) or discarded according to the matching rule in the ACL. If no matching rule is found, the packet is passed.

The packets meeting the requirement will be permited to go through Packet Interface, or else they will be denied access]

FDP_IFF.1.3 The TSF shall enforce the **[following additional rules: none].**

FDP_IFF.1.4 The TSF shall explicitly authorise 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:**[**

- **For ACL feature, packets that match configured ACL with action “deny” are dropped]**

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***[3 consecutive]*** unsuccessful authentication attempts occur related to **[user logging in]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall **[terminate the session of the authentication user and block the logging in of the corresponding user for 5 minutes]**.

6.2.4.2 FIA_ATD.1 User attribute definition

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

[

1. **user ID**
2. **user level**
3. **password**
4. **temporary blocking time for user accounts after unsuccessful authentication attempts**
5. **time when users are logging in**
6. **max idle time (maximum time of inactivity before finishing the user session)]**

Application Note: A User ID is generated in AAA server and is assigned to a user once logged in. User ID is released when a user goes offline.

Username is the name of the account while User ID is the corresponding identifier each time the username is used to login the system, the maximum number of the identifiers (instance) a username is allowed to have is configurable. E.g. a User ID of 2 stands for 2 users using the same account logged in the system.

6.2.4.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for user authentication for SSH and they are case sensitive. All passwords should be longer than 7 characters and contain at least one lower-case letter, one upper-case letter, one number and one special character.]**

6.2.4.4 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **[establishment of a secure remote session between the administrative user and the TOE component]** on behalf of the user to be performed before the user is authenticated.

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

6.2.4.5 FIA_UAU.5 Multiple authentication mechanisms

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

1. **User authentication by password and/or**
2. **User Authentication by RSA/DSA keys]**

to support user authentication.

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

1. **verification of stored credential in the local database for user password authentication**
2. **verification of stored RSA/DSA keys for asymmetric authentication].**

6.2.4.6 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **[establishment of a secure remote session between the administrative user and TOE component]** on behalf of the user to be performed before the user is identified.

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

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***[determine the behavior of]*** the functions **[defined in FMT_SMF.1]** to **[the administrator-defined roles]**

6.2.5.2 FMT_MSA.1/VRP Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[VRP access control policy]** to restrict the ability to ***[query, modify]*** the security attributes **[user ID, user level]** to the **[role Administrator (not including Operator and Maintainer) listed in FMT_SMR.1].**

6.2.5.3 FMT_MSA.1/ACLs Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[ACLs flow policy]** to restrict the ability to ***[query, modify]*** the security attributes **[security attributes defined in FDP_IFF.1]** to the **[roles Administrator and Maintainter included in FMT_SMR.1].**

6.2.5.4 FMT_MSA.3/VRP Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[VRP access control policy]** to provide ***[restrictive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **[role Administrator (not including Operator and Maintainer) listed in FMT_SMR.1]** to specify alternative initial values to override the default values when an object or information is created.

Application note: The user level when a user is created is fixed by design and it is always the more restrictive (less privileges). The user level cannot be modified during the creation of the user but once it has been created.

6.2.5.5 FMT_MSA.3/ACLs Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[ACLs flow policy]** to provide ***[permissive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **[oles Administrator and Maintainter included in FMT_SMR.1]** to specify alternative initial values to override the default values when an object or information is created.

Application note: Information flow control is fixed by design and by default the traffic is passed if no rules are created (permissive). The behaviour can be restricted by creating new ACL rules.

6.2.5.6 FMT_SMF.1 Specification of Management Functions

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

1. **authentication, authorization ,encryption policy**
2. **ACL policy**
3. **user management**
4. **port security**
5. **The maximum number of user logins**
6. **Configure the interval for user inactivity for the termination of an established session]**

6.2.5.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[**

User role: Every

Administrator roles: Operator, Maintainer and Administrator]

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

Additional note: The groups “Every, Operator, Maintainer and Administrator” are named as “every, oper, main and admin” when they are used in the TOE.

6.2.6 TOE access (FTA)

6.2.6.1 FTA_SSL.3 TSF-initiated termination

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

6.2.6.2 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 doesn’t match IP address configured in ACL for user management.]**

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_TRP.1 Trusted path

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[remote management]**.

6.3 Security Functional Requirements Rationale

6.3.1 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

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

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

Table 6-1 Dependencies between TOE Security Functional Requirements

Security Functional Requirement	**Dependencies**	**Resolution**
FAU_GEN.1	FPT_STM.1	Timestamps are provided by the environment (by the underlying operative system RTOS)
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/AES Cryptographic key generation Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FCS_COP.1/RSA Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA Cryptographic key generation Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.

Security Functional Requirement	Dependencies	Resolution
FCS_COP.1/ SHA2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	SHA2 is a cryptographic operation that does not require generate or destroy keys
FCS_COP.1/DSA Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DSA Cryptographic key generation Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FCS_CKM.1/RSA Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/RSA Cryptographic operation Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.

Security Functional Requirement	**Dependencies**	**Resolution**
FCS_CKM.1/DSA Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DSA Cryptographic operation Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FCS_CKM.1/AES Cryptographic key destruction	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4]	FCS_COP.1/AES Cryptographic operation Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3/VRP
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3/ACLs
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No Dependencies	None
FIA_SOS.1	No Dependencies	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1

Security Functional Requirement	Dependencies	Resolution
FIA_UAU.5	No Dependencies	None
FIA_UID.1	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/VRP	[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/ACLs	[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/VRP	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/VRP FMT_SMR.1
FMT_MSA.3/ACLs	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ACLs FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_TRP.1	No Dependencies	None

6.3.2 Sufficiency and coverage

Table 6-2 Objectives to SFR mapping rationale

Objective	SFRs	Rationale
O.Communication	FTP_TRP.1	This SFR provides the secure communication between users and management interface of the TOE
	FIA_SOS.1	These SFRs provide the secure communication between TOE and PC and ensure that the secrets for this are strong enough.
	FCS_COP.1/* FCS_CKM.1/*	These SFRS provide the cryptographic services for the secure communication above.
O.Forwarding	FDP_IFC.1 FDP_IFF.1	These SFRs apply ACL to both packets going to the forwarding Plane and through the TOE and thereby ensure that only accepted traffic goes through.
O.Authentication	FIA_UID.1 FIA_UAU.1 FIA_UAU.5	These SFRs ensure that a user must identify and authenticate himself by local password.
	FTA_TSE.1 FIA_AFL.1 FTA_SSL.3	• The SFRs support authentication by: • Refusing logins from certain IP addresses • Not allowing unlimited login attempts • Logging out users after an inactivity period
O.Authorisation	FDP_ACC.1 FDP_ACF.1	These SFRs ensure that only properly authorized users can access certain functions
	FMT_SMR.1 FIA_ATD.1	These SFRs defines authorization levels and ensure that upon login an user gets the proper authorization level.
	FMT_MOF.1 FMT_SMF.1	These SFR lists certain management functions and restricts them to the proper authorization level.
	FMT_MSA.1/VRP FMT_MSA.1/ACLs FMT_MSA.3/VRP FMT_MSA.3/ACLs	These SFRs ensure that new admins are able to configure and manage control and flow policies.

Objective	SFRs	Rationale
O.Audit	FAU_GEN.1, FAU_GEN.2	These SFRs ensure that audit records can be generated of significant events and that these contain useful information, including the correct time of the events.
	FAU_SAR.1	These SFRs ensure that the correct users can read the correct information from the audit records.
	FAU_STG.1, FAU_STG.3	These SFRs ensure the audit data is protected against unauthorized modification and deletion, and what happens when audit storage fills up.

6.4 Security Assurance Requirements

The Evaluation Assurance Level 3 has been chosen to commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL package selected (EAL3) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here.

Assurance Class	Assurance Component
ADV	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.2

6.5 Security Assurance Requirements Rationale

ASE_REQ.2.8C *The security requirements rationale shall explain why the SARs were chosen.*

The Evaluation Assurance Level 3 has been chosen to commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 Authentication

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

Table 7-1 SFR to TSF mapping

SFR	TSF
FIA_AFL.1	Support max attempts due to authentication failure within certain period of time. This function is achieved by providing counts on authentication failure.
FIA_ATD.1	Support for user individual attributes in order to achieve all the enumerated features: user ID, user level, and password, temporary blocking time for user accounts after unsuccessful authentication attempts, time when users are logging in. A User ID is generated in AAA server and is assigned to a user once logged in. User ID is released when a user goes offline. Username is the name of the account while User ID is the corresponding identifier each time the username is used to login the system, the maximum number of the identifiers (instance) a username is allowed to have is configurable. E.g. a User ID of 2 stands for 2 users using the same account logged in the system.
FIA_SOS.1	The TOE supports a mechanism to verify that secrets meet that password used as seeds for user authentication for SSH are case sensitive.
FIA_UAU.1	SSH session is established after authentication.
FIA_UAU.5	Support authenticate user login using SSH, by password authentication, DSA/RSA authentication, or combination. This function is achieved by performing

	authentication for SSH user.
FIA_UID.1	The TOE supports the establishment of a secure remote session between the administrative user and TOE component on behalf of the user to be performed before the user is identified. The TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
FTA_SSL.3	Support logout when no operation is performed on the user session within a given interval. This function is achieved by performing count-down through timing related to clock function.
FTA_TSE.1	The TOE supports deny sessions based on the number of authentication failures. 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.
FTP_TRP.1	The TOE provides a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure. The TOE permits remote users to initiate communication via the trusted path and requires the use of the trusted path for remote management.

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

7.2 Access Control

The TOE enforces an access control by supporting following functionalities:

1. Support 4 access levels. This function is achieved by storing number as level in memory.
2. Support assigning access level to commands. This function is achieved by associating access level number with commands registered.
3. Support assigning access level to user ID. This function is achieved by associating access level number with user ID.
4. Support limiting executing commands of which the access level is less or equal to the level of user. This function is achieved by performing an

evaluation that level of commands is less or equal to level of user. This limitation of access also prevents users from accessing or deleting log files if they have insufficient rights.

(FDP_ACC.1, FDP_ACF.1, FMT_SMR.1)

7.3 ACL

The TOE supports Access Control Lists (ACLs) to filter traffic destined to be forwarded by the TOE.
1. The TOE supports ACLs, which are based on the upper-layer protocol number, the source and destination IP addresses, the source and destination port numbers, and the packet direction.
2. The TOE permits an information flow between controlled subjects if all information security attributes are permitted by ACL. Packets not matching the ACL are logged and discarded by the router.
3. The TOE restricts the ability to read, modify and delete entries in ACLs to users with sufficient access rights.
4. A basic ACL matches packets only based on the source IP address, fragment flag, and time range.
(FDP_IFC.1, FDP_IFF.1)

7.4 Auditing

The TOE can provide auditing ability by receiving all types of logs and processing them according to user's configuration:

Table 7-2 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	Only users with the required user level can query operation logs and security logs.
FAU_STG.1	The operation logs and security logs do not allow 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.

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

7.5 Communication Security & Cryptographic functions

The TOE provides communication security by implementing SSH protocol. The SSHv2 (SSH2.0) is implemented and it is recommended for most cases by providing more secure and effectiveness in terms of functionality and performance.

1. Support SSHv2. This function is achieved by providing implementation of SSHv2.
2. Support diffie-hellman as key exchange algorithm of SSH. This function is achieved by providing implementation of diffie-hellman-group-exchange-sha256 algorithm.
3. Support AES encryption algorithm. This function is achieved by providing implementation of AES-CTR algorithm.
4. Support SHA2 verification algorithm. This function is achieved by providing implementation of SHA2-256 algorithm.
5. The TOE supports asymmetric authentication using the RSA/DSA algorithms with a key length of 2048 bits for SSH.

(FCS_CKM.1/*, FCS_COP.1/*, FTP_TRP.1)

7.6 Security Management

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes:

- User management, including user name, passwords, etc.
- Enabling/disabling of SSH for the communication between PC clients and the TOE.
- Defining IP addresses and address ranges for clients that are allowed to connect to the TOE.

All of these management options are typically available via the PC.

Detailed function specification include following:

1. Support remotely managing the TOE using SSH.
2. Support configuration on service port for SSH;
3. Support configuration on RSA/DSA key for SSH;
4. Support configuration on encryption algorithm for SSH;
5. Support configuration on logout when no operation is performed on the user session within a given interval;
6. Support configuration on max attempts due to authentication failure within certain period of time;
7. Support configuration on limiting access by IP address;
8. Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;

Above functions are achieved by providing interpreting input commands and storing result of interpreting in memory.

(FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/VRP, FMT_MSA.1/ACLs, FMT_MSA.3/VRP, FMT_MSA.3/ACLs)

A Abbreviations, Terminology and References

A.1 Abbreviations

CC	Common Criteria
CLI	Command Line Interface
GUI	Graphical User Interface
LPU	Line Process Unit
MPU	Main Process Unit
NE	Network Element
OFC	Optical Flexible Card
PTN	Packet Transport Network
PP	Protection Profile
SFE	Switch Fabric Extend unit
SFR	Security Functional Requirement
SFU	Switch Fabric Unit
SPU	Service Process Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
AES	Advanced Encryption Standard
XCS	Cross-connect and Synchronous Timing Board
RTOS	Real Time Operating System
RSA	Rivest-Shamir-Adleman
DSA	Digital Signature Algorithm

A.2 References

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

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, August 2017