



HUAWEI NE20E series Router  
V800R010C10  
& NE08E series Router  
V300R003C10  
Security Target

Version: 3.0  
Last Update: 2019-04-08  
Author: HUAWEI Technologies Co., Ltd.

## Table of Contents

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>1 INTRODUCTION .....</b>	<b>4</b>
1.1 Security Target Identification .....	4
1.2 TOE Identification .....	4
1.3 Target of Evaluation (TOE) Overview .....	4
1.4 TOE Description .....	5
1.4.1 Architectural overview .....	5
1.4.2 Physical scope.....	8
1.4.3 Logical scope.....	22
1.4.4 TSF and Non-TSF data.....	25
<b>2 CC CONFORMANCE CLAIM .....</b>	<b>27</b>
<b>3 TOE SECURITY PROBLEM DEFINITION.....</b>	<b>28</b>
3.1 Threats.....	28
3.2 Assumptions .....	28
3.2.1 Environment of use of the TOE .....	28
<b>4 SECURITY OBJECTIVES .....</b>	<b>29</b>
4.1 Objectives for the TOE.....	29
4.2 Objectives for the Operational Environment .....	30
4.3 Security Objectives Rationale.....	30
<b>5 EXTENDED COMPONENTS DEFINITION .....</b>	<b>32</b>
<b>6 SECURITY REQUIREMENTS.....</b>	<b>33</b>
6.1 Conventions.....	33
6.2 TOE Security Functional Requirements.....	33
<b>6.2.1 Security Audit (FAU) .....</b>	<b>33</b>
6.2.2 Cryptographic Support (FCS) .....	34
6.2.3 User Data Protection (FDP) .....	37
6.2.4 Identification and Authentication (FIA).....	40
6.2.5 Security Management (FMT).....	42
6.2.6 Protection of the TSF (FPT).....	44

6.2.7 TOE access (FTA).....	44
6.2.8 Trusted Path/Channels (FTP).....	44
6.3 Security Functional Requirements Rationale .....	45
6.3.1 Security Requirements Dependency Rationale.....	45
6.3.2 Sufficiency and coverage .....	48
6.4 Security Assurance Requirements.....	49
6.5 Security Assurance Requirements Rationale.....	49
<b>7 TOE SUMMARY SPECIFICATION.....</b>	<b>49</b>
7.1 TOE Security Functional Specification.....	49
7.1.1 Authentication.....	49
7.1.2 Access Control .....	50
7.1.3 Traffic Forwarding .....	50
7.1.4 Auditing .....	51
7.1.5 Communication Security .....	52
7.1.6 ACL.....	52
7.1.7 Security Management .....	53
7.1.8 Denial-of-Service Protection .....	54
7.1.9 Cryptographic functions .....	54
7.1.10 Time.....	55
7.1.11 SNMP Trap.....	55
<b>8 ABBREVIATIONS, TERMINOLOGY AND REFERENCES .....</b>	<b>56</b>
8.1 Abbreviations .....	56
8.2 Terminology.....	57
8.3 References.....	57

# 1 Introduction

This Security Target is for the evaluation of HUAWEI NE20E series Router V800R010C10 and NE08E series Router V300R003C10.

## 1.1 Security Target Identification

Name: HUAWEI NE20E series Router V800R010C10 & NE08E series Router V300R003C10 Security Target

Version: 3.0

Publication Date: 2019-04-08

Author: HUAWEI Technologies Co., Ltd.

## 1.2 TOE Identification

Name: Huawei NE20E series Router V800R010C10 and NE08E series Router V300R003C10

Version: V800R010C10 and V300R003C10

Revision: SPC500

Developer: HUAWEI Technologies Co., Ltd.

Keywords: HUAWEI, VRP, Versatile Routing Platform, Service Routers

## 1.3 Target of Evaluation (TOE) Overview

Huawei NetEngine20E-S Universal Service Router (NE20E) series is medium- or high-end network product developed by Huawei for transportation, finance, energy, government, education, enterprise, and Internet service provider (ISP) networks. The NE20E series routers mainly serve as aggregation nodes on wide area networks (WANs) and egress nodes on enterprise or campus networks.

An NE08E device is generally located at the intersection between an enterprise's internal network and an external network. An NE08E is the only entrance and exit of data flows between the internal and external networks. An NE08E can bear multiple types of services, greatly reducing network construction investment and long-term operation and maintenance costs of an enterprise network. As a part of the all-IP solution for a Huawei power network, NE08E devices are deployed between substations/power plants and IP aggregation routers and provide data access services for the substations/power plants.

The NE20E Series Routers can be flexibly deployed at the access and aggregation layer of IP/MPLS networks and work with other NE routers to provide an all-around network solution for enterprise users, satisfying diversified service requirements in the future.

The NE08E adopts an advanced routing architecture and a uniform platform to receive, transmit, and bear multiple types of services on an all-IP network. This improves network flexibility and transmission efficiency, helps construct reliable carrier-class packet transport networks (PTNs), and reduces the total cost of ownership (TCO).

The NE20E-S series and NE08E series routers run on the Versatile Routing Platform (VRP) operating system and use Huawei-developed NP chips and hardware-based forwarding and non-blocking switching technologies. VRP provides extensive security features. These features include assigning different privileges to administration users

with different privilege levels; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

The types of boards on the NE20E and NE08E are MPU, NSP and PIC. The Main Processing Units (MPU) integrate the main control unit and the system maintenance unit. The MPU controls and manages the system in a centralized way and is responsible for data exchange. The Network Service Processor (NSP) and Physical Interface Card (PIC) are the actual hardware providing network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions downloaded from VRP. Besides the MPUs, NSPs and PICs, there are other type of boards on TOE, such as Power Boards and FAN Boards. Only MPU is security relevant.

The environment for TOE comprises the following components:

- An optional Radius or TACACS+ server providing authentication and authorization decisions to the TOE.
- Peer routers providing routing information to the TOE via dynamic protocols, such as BGP, OSPF and IS-IS.
- Peer routers providing LSP information to the TOE via dynamic protocols, such as LDP
- Local PCs used by administrators to connect to the TOE for access of the command line interface through TOE's ETH interface via a secure channel enforcing SSH.
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through interfaces on Interface boards within the TOE via a secure channel enforcing SSH.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.

## 1.4 TOE Description

### 1.4.1 Architectural overview

This section will introduce the HUAWEI NE20E series Router V800R010C10SPC500 and NE08E series Router V300R003C10SPC500 from a physical architectural view and a software architectural view.

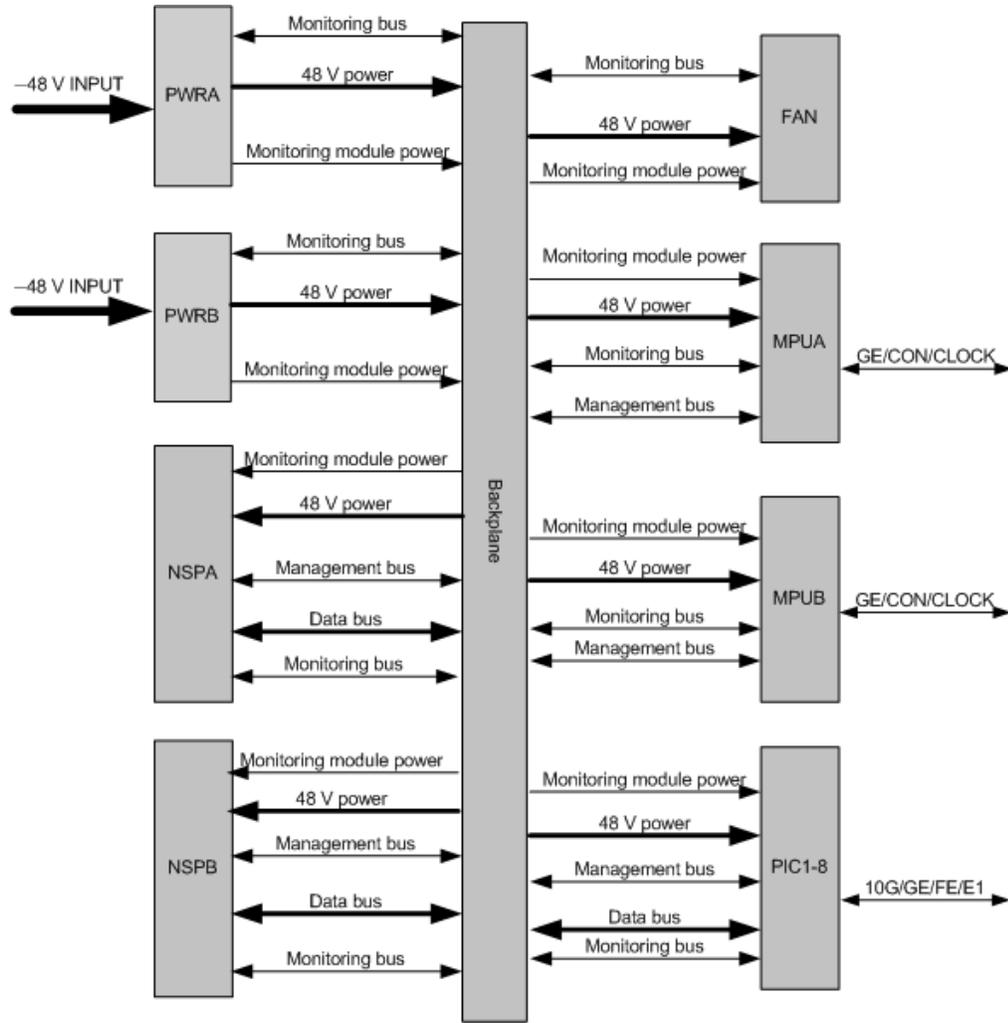
#### 1.4.1.1 Physical Architecture

A system consists of the following systems:

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

The functional host system is composed of the system backplane, MPUs, NSPs, and PICs. It connects to the NMS through NMS interfaces. The functional host system processes data and monitors and manages the power distribution system and heat dissipation system. The functional host system consists of the system backplane, MPUs, NSPs, and PICs as depicted in **Figure 1**

**Functional host system.**



**Figure 1 Functional host system**

**1.4.1.2 Software Architecture**

The NE20E and NE08E series routers provide a multi-process and full-service software architecture that is reliable, scalable, and flexible.

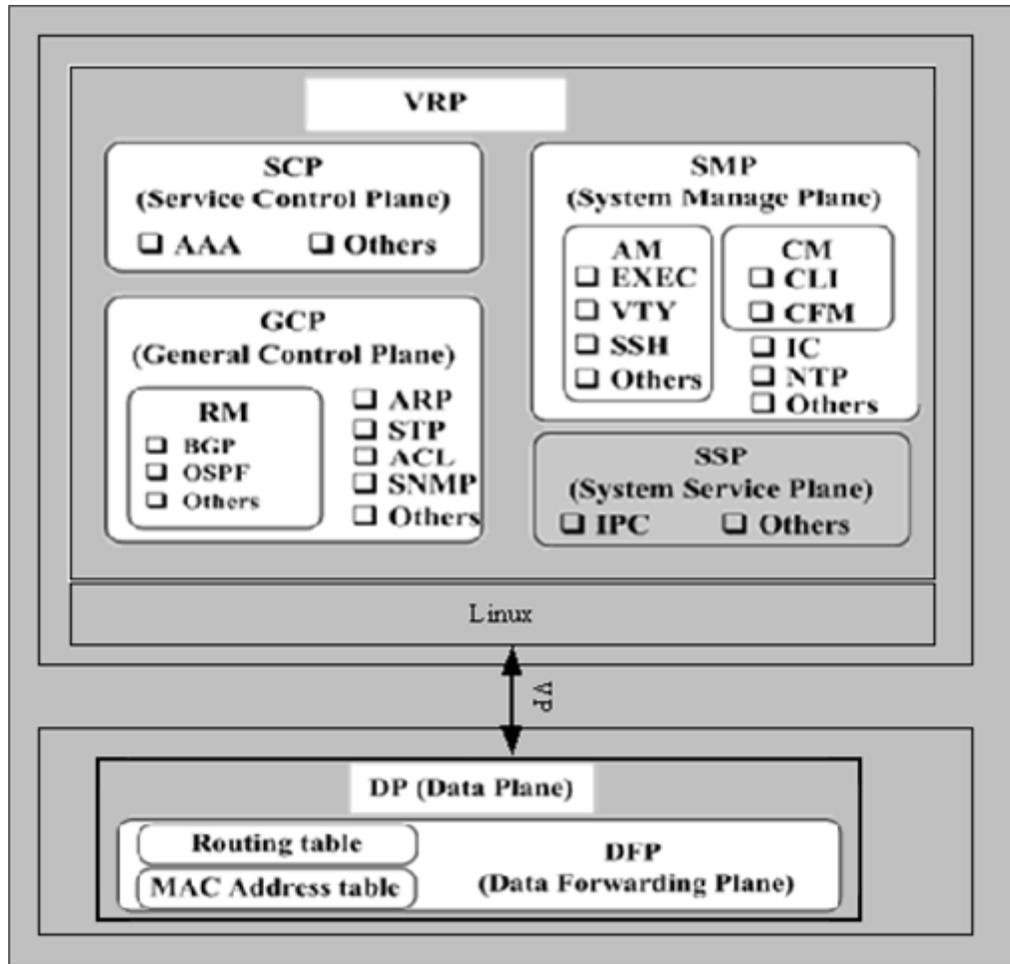


Figure 2: TOE Software architecture

The TOE's software architecture consists of three logical planes to support centralized forwarding and control and distributed forwarding mechanism.

- Data plane
- Control and management plane
- Monitoring plane

Note that the **monitoring plane** is to monitor the system environment by detecting the voltage, controlling power-on and power-off of the system, and monitoring the temperature and controlling the fan. The monitoring plane is not considered to be security-related.

The **control and management plane** is the core of the entire system. It controls and manages the system. The control and management unit processes protocols and signals, configures and maintains the system status, and reports and controls the system status.

The **data plane** is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or decapsulates packets, forwards IPv4/IPv6 packets, performs Quality of Service (QoS) and scheduling, completes inner high-speed switching, and collects statistics.

**The VRP** is the control and management platform that runs on the router. The VRP supports IPv4/IPv6, and routing protocols such as Border Gateway Protocol (BGP),

Open Shortest Path First (OSPF), calculates routes, generates forwarding tables, and delivers routing information to the Data Plane (DP). The VRP includes Service Control Plane (SCP), System Management Plane (SMP), General Control Plane (GCP) and other TSF and non-TSF sub-systems.

### 1.4.2 Physical scope

This section will define the physical scope (table 1) of the HUAWEI NE20E series Router V800R010C10 and NE08E series Router V300R003C10 to be evaluated.

The physical boundary of the TOE is the actual router system itself -- in particular, the functional host system. The power distribution system and heat dissipation system are part of the TOE but not to be evaluated because they are security irrelevant.

There are two types of chassis of NE20E as shown in Table 2.

There are one type of chassis of NE08E as shown in Table 4.

TYPE	Delivery Item	Version
Hardware	<p>There are two types of chassis of NE20E as shown in Table 2.</p> <p>There are one type of chassis of NE08E as shown in Table 4.</p> <p>Info:</p> <p>We cooperate with world class logistics service providers such as DHL, KN, Schenker, Panalpina and so on to ensure the security of product in international transportation and regional warehousing, so as to deliver products to customers efficiently and securely</p>	NA
Software	<p>NE20E series Router V800R010C10SPC500</p> <p>Format: V800R010C10SPC500-NE20E-NSP-50-120-A-B.cc</p> <p>Info:</p> <p>Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE.</p> <p>Users can verify the software by digital signature(The digital signature is also published on HUAWEI support website)</p> <p>-----BEGIN PGP SIGNATURE-----</p> <p>Version: GnuPG v2.0.19 (GNU/Linux)</p> <p>iQEcBAABCAAGBQJbjRF8AAoJEJmtgd8np0gkPW sH/RUyJMZNTscQYMN3HNRyxXHi cGwYgJPZoz1rugw58UiIDsA50UCURhhmfOG98xZ</p>	V800R010C10 SPC500

	<p>DdoUaAXYWY1WU8/hNfYFs6/S5  pf81RaC4PTL8vb1i0RfZ8S1D0dO5S6bLH/zzWg01  ciMoH6ZcRjTWtxPCVPHuMNxQ  vIUkV6+UQjhL2jgcmTJAThwWwyFg2T+5vxeV8m9  HNSnA93acbouALTeMGc7VVzT2  hpkpxPyL5Eg8ayRbWQsKCCSMkLle6PsLEGpSG+  mLwLnIr3JFNZPTZYBGWBQ60SJz  /kcdN/0RbF3Fpfckot8XI+8rdkC9Z3i6ZAI6tqIM/cZ+A  H+yHaFesHEaWJmvRgk=  =//SI  -----END PGP SIGNATURE-----</p>	
	<p>NE08E series Router V300R003C10SPC500</p> <p>Format:  V300R003C10SPC500-NE-08E-S6E.cc</p> <p>Info:  Users can login the HUAWEI support website to  download the software packet in accordance to the  version of the TOE.  Users can verify the software by digital  signature(The digital signature is also published on  HUAWEI support website)  -----BEGIN PGP SIGNATURE-----  Version: GnuPG v2.0.19 (GNU/Linux)</p> <p>iQEcBAABCAAGBQJbihZcAAoJEJmtgd8np0gkiEsH  /1SUZgMqTjo/15iqAM2cWPpf  rsVS2MlyhsHkvmn33kUe/M2LvLS0M1QUPgGto81  YJzAIPSy5P1hLQRWRK3+OZqp1  OVFziPBh15ZzGkmgEy7eUK1S0IBX2jWrHLDImN/g  US/gx12RSwkqZg9ZywWqb7tZ  EiYIGzulFZlh65j2q2EvYfkTTJiAMrwiJjJN7tySSZa8  wsaZ7ulNSwjWnbS75GP4  a3WrRfsT2YlbMj3u61V8MGohRTskGcPFh/lckaEm  MiK8TsA0oeqasrCsuVRLGXUw  KcsAZVMKH3Xz6/kJDckf+zn8XJTGvGlo5+KLJkLI  dAKnf3GCC23HCMWly8M+aXE=  =kMzE  -----END PGP SIGNATURE-----</p>	<p>V300R003C10  SPC500</p>
<p>Product  guidance</p>	<p>Huawei NE20E&amp;NE08E Common Criteria Security  Evaluation - Certified Configuration</p> <p>Info:  The documentation is delivered as PDF on a</p>	<p>2.1</p>

	<p>CD-ROM if the customer requests it.</p> <p>SHA256 checksum: 342f734d94af1819a183c28278bd3c4a071a027af70 b454fb89798be838eafe6</p>	
	<p>NE20E V800R010C10 Product Documentation 01</p> <p>Info: Users can login the HUAWEI support website to read the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website.</p>	V800R010C10
	<p>NE08E V300R003C10 Product Documentation 01</p> <p>Info: Users can login the HUAWEI support website to read the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website.</p>	V300R003C10

**Table 1** Physical scope

The following boards will be covered during this evaluation (● means related):

Model	Description	NE20E-S8A	NE20E-S16A
CR2D0MPUE110	Main Processing Unit E1	●	●
CR2D0NSP5010	Network Service Processor (NSP-50)	●	●
CR2DNSPE5010	Network Service Processor (NSP-50-E)	●	●
CR2DNSP12010	Network Service Processor (NSP-120)	●	●
CR2DNSP1201E	Network Service Processor (NSP-120-E)	●	●
CR2DNSPA0010	Network Service Processor (NSP-A)	●	●
CR2DNSPB0010	Network Service Processor (NSP-B)	●	●
CR2DNSPC0010	Network Service Processor (NSP-C)	●	●
CR2DNSPD0010	Network Service Processor (NSP-D)	●	●
CR2D00E1NC10	1-Port 100GBase-CFP2 Physical Interface Card (PIC)	●	●
CR2D00LAXF10	10-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●
CR2D00E1MF70	1-Port 40GBase-CFP Physical Interface Card (PIC)	●	●

Model	Description	NE20E-S8A	NE20E-S16A
CR2D00L4XF11	4-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●
CR2DL1XE8G11	1-Port 10GBase LAN/WAN-SFP+ + 8-Port 100/1000Base-X-SFP Physical Interface Card	●	●
CR2D00L2XF12	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●
CR2D00L4XF10	4-Port 10GBase LAN-SFP+ Physical Interface Card	●	-
CR2DL1XE8G10	1-Port 10GBase LAN/WAN-SFP+ + 8-Port 100/1000Base-X-SFP Physical Interface Card	●	●
CR2D00L2XF11	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●
CR2D0L2XFH10	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card H	●	●
CR2D0L2XFH11	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card H (PIC-H)	●	●
CR2D00E8GE12	8-Port 100/1000Base-RJ45 Physical Interface Card	●	●
CR2D00EAGF10	10-Port 100/1000Base-X-SFP Physical Interface Card	●	●
CR2D00E8GF11	8-Port 100/1000Base-X-SFP Physical Interface Card	●	●
CR2D00E8GE11	8-Port 100/1000Base-RJ45 Physical Interface Card	●	●
CR2D0EAGFH10	10-Port 100/1000Base-X-SFP Physical Interface Card H	●	●
CR2D0E8GFH10	8-Port 100/1000Base-X-SFP Physical Interface Card H (PIC-H)	●	●
CR2D00EEGF10	20-Port 100/1000Base-X-SFP Physical Interface Card(PIC)	-	●
CR5D08CWDM70	8-Channel CWDM Multiplexing & Demultiplexing (1471/1491/1511/1531/1551/1571/1591/1611nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M01	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1471nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M02	Bidirectional 1-Channel CWDM Optical Add/Drop	●	●

Model	Description	NE20E-S8A	NE20E-S16A
	Multiplexing (1491nm) Physical Interface Card(PIC)		
CR5D1DMD1M03	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1511nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M04	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1531nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M05	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1551nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M06	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1571nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M07	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1591nm) Physical Interface Card(PIC)	●	●
CR5D1DMD1M08	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1611nm) Physical Interface Card(PIC)	●	●
CR5D2DMD2M01	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1471/1491nm) Physical Interface Card(PIC)	●	●
CR5D2DMD2M02	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1511/1531nm) Physical Interface Card(PIC)	●	●
CR5D2DMD2M03	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1551/1571nm) Physical Interface Card(PIC)	●	●
CR5D2DMD2M04	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1591/1611nm) Physical Interface Card(PIC)	●	●
CR2D000IE110	32-Port E1 Physical Interface Card(75ohm)	●	●
CR2D000IE111	32-Port E1 Physical Interface Card(120ohm)	●	●
CR2D000DE110	16-Port E1 Physical Interface Card(PIC, 75ohm) ,High anti-corrosion	●	●
CR2D000DE111	16-Port E1 Physical Interface Card(120ohm)	●	●
CR2D00A2CF10	2-Port OC-3c/STM-1c ATM-SFP Physical Interface	●	●

Model	Description	NE20E-S8A	NE20E-S16A
	Card(PIC)		
CR2D00C4CF11	4-Port Channelized STM-1c POS-SFP Physical Interface Card	●	●
CR2D00P4CF11	4-Port OC-3c/STM-1c POS-SFP Physical Interface Card	●	●
CR2DP2C1HF11	2-Port OC-3c/STM-1c (or 1-Port OC12c/STM-4C) POS-SFP Physical Interface Card	●	●
CR2D00C1CF11	1-Port Channelized STM-1c POS-SFP Physical Interface Card	●	●
CR5D3DMR4M01	4-Channel CWDM Optical Add/Drop Multiplexing (1471/1491/1511/1531nm) Physical Interface Card(PIC)	●	●
CR5D3DMR4M02	4-Channel CWDM Optical Add/Drop Multiplexing (1551/1571/1591/1611nm) Physical Interface Card(PIC)	●	●
CR2D00EEGF11	20-Port 100/1000Base-X-CSFP Physical Interface Card(PIC)	●	●
CR2D0EAGFE10	10-Port 100/1000Base-X-SFP Physical Interface Card E(PIC-E)	●	●
CR2D0L2XFE10	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card E(PIC-E)	●	●
CR5D00AUXQ10	Auxiliary Flexible Interface Card with 4-Port 100Base-RJ45 (FIC, Supporting 1588v2)	●	●
CR2D00MPAA90	4-Channel FXS/FXO+2-Channel E&M+2-Channel RS232+2-Channel RS485 Board	●	●
CR2D00MP8A90	4 Channels C37.94 Optical Interface and 4 Channels CoDir64K Electric Interface Board	●	●
CR2D000SA890	8-Channel V. 35/X. 21/V. 24 Board	●	●
CR2D0E5XMF10	2-Port 50GBase/1-Port 100GBase-QSFP28 Physical Interface Card(PIC)	●	●
CR2D00E2NF10	2-Port 100GBase-QSFP28 Physical Interface Card(PIC)	●	-
CR2D00E1NC11	1-Port 100GBase-CFP2Physical Interface Card(PIC)	●	●
CR2D00LAXF11	10-Port 10GBase LAN/WAN-SFP+ Physical Interface Card(PIC)	●	●
CR5D00E4XF20	4-Port 10GBase-SFP+MACsec Interface Card	●	●

Model	Description	NE20E-S8A	NE20E-S16A
CR5D00E1NB20	1-Port 100GBase-QSFP28+MACsec Interface Card	●	●
CR5DE2NE4X10	2-Port 100GBase-QSFP28/1-Port100GBase-QSFP28+4-Port 10GBase-SFP+MACsec Interface Card	●	●
CR2D0EM4TP10	4 Channels GE/FE PoE Electrical Interface Board	●	●
CR2D000EM890	6 Channels E&M Interface Board	●	●
CR2D000DE110	16-Port E1 Physical Interface Card(PIC, 75ohm) ,High anti-corrosion	●	●

**Table 2** List of boards of NE20E

The following subcards on the NSP will be covered during this evaluation (● means related):

Model	Description	NSP -50	NSP- 50-E	NSP -12 0	NSP-1 20-E	NS P- A	NS P- B	NS P- C	NS P- D
CR2D00 E1NC10	1-Port 100GBase-CFP2 Physical Interface Card(PIC)	-	-	-	-	-	-	●	-
CR2D00 LAXF10	10-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	-	-	-	-	-	-	●	-
CR2D00 E1MF70	1-Port 40GBase-CFP Physical Interface Card(PIC)	-	-	●	●	●	●	●	●
CR2D00 L4XF11	4-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●	●	●	●	●	●	●
CR2DL1 XE8G11	1-Port 10GBase LAN/WAN-SFP+ + 8-Port 100/1000Base-X-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 L2XF12	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●	●	●	●	●	●	●

Model	Description	NSP-50	NSP-50-E	NSP-120	NSP-120-E	NSP-A	NSP-B	NSP-C	NSP-D
CR2D00 L4XF10	4-Port 10GBase LAN-SFP+ Physical Interface Card	-	-	●	●	●	●	●	●
CR2DL1 XE8G10	1-Port 10GBase LAN/WAN-SFP+ + 8-Port 100/1000Base-X-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 L2XF11	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card	●	●	●	●	●	●	●	●
CR2D0L 2XFH10	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card H	●	●	●	●	●	●	-	-
CR2D0L 2XFH11	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card H (PIC-H)	-	-	-	-	●	●	●	●
CR2D00 E8GE12	8-Port 100/1000Base-RJ45 Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 EAGF10	10-Port 100/1000Base-X-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 E8GF11	8-Port 100/1000Base-X-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 E8GE11	8-Port 100/1000Base-RJ45 Physical Interface Card	●	●	●	●	●	●	●	●
CR2D0E AGFH10	10-Port 100/1000Base-X-SFP Physical Interface Card H	●	●	●	●	●	●	-	-
CR2D0E 8GFH10	8-Port 100/1000Base-X-SFP Physical Interface Card H (PIC-H)	-	-	-	-	●	●	●	●
CR2D00 EEGF10	20-Port 100/1000Base-X-SFP	-	-	●	●	●	●	●	●

Model	Description	NSP -50	NSP- 50-E	NSP -12 0	NSP-1 20-E	NS P- A	NS P- B	NS P- C	NS P- D
	Physical Interface Card(PIC)								
CR5D08 CWDM70	8-Channel CWDM Multiplexing & Demultiplexing (1471/1491/1511/1531/1551/1571/1591/1611nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M01	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1471nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M02	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1491nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M03	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1511nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M04	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1531nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M05	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1551nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●

Model	Description	NSP -50	NSP- 50-E	NSP -12 0	NSP-1 20-E	NS P- A	NS P- B	NS P- C	NS P- D
CR5D1D MD1M06	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1571nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M07	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1591nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D1D MD1M08	Bidirectional 1-Channel CWDM Optical Add/Drop Multiplexing (1611nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D2D MD2M01	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1471/1491nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D2D MD2M02	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1511/1531nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D2D MD2M03	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1551/1571nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●
CR5D2D MD2M04	Bidirectional 2-Channel CWDM Optical Add/Drop Multiplexing (1591/1611nm) Physical	●	●	●	●	●	●	●	●

Model	Description	NSP -50	NSP- 50-E	NSP -12 0	NSP-1 20-E	NS P- A	NS P- B	NS P- C	NS P- D
	Interface Card(PIC)								
CR2D00 0IE110	32-Port E1 Physical Interface Card(75ohm)	●	●	●	●	●	●	●	●
CR2D00 0IE111	32-Port E1 Physical Interface Card(120ohm)	●	●	●	●	●	●	●	●
CR2D00 0DE110	16-Port E1 Physical Interface Card(PIC, 75ohm) ,High anti-corrosion	●	●	●	●	●	●	●	●
CR2D00 0DE111	16-Port E1 Physical Interface Card(120ohm)	●	●	●	●	●	●	●	●
CR2D00 A2CF10	2-Port OC-3c/STM-1c ATM-SFP Physical Interface Card(PIC)	●	●	●	●	●	●	-	-
CR2D00 C4CF11	4-Port Channelized STM-1c POS-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 P4CF11	4-Port OC-3c/STM-1c POS-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2DP2 C1HF11	2-Port OC-3c/STM-1c (or 1-Port OC12c/STM-4C) POS-SFP Physical Interface Card	●	●	●	●	●	●	●	●
CR2D00 C1CF11	1-Port Channelized STM-1c POS-SFP Physical Interface Card	●	●	●	●	●	●	-	●
CR5D3D MR4M01	4-Channel CWDM Optical Add/Drop Multiplexing (1471/1491/1511/1531nm) Physical Interface Card(PIC)	●	●	●	●	●	●	●	●

Model	Description	NSP -50	NSP- 50-E	NSP -12 0	NSP-1 20-E	NS P- A	NS P- B	NS P- C	NS P- D
CR5D3D MR4M02	4-Channel CWDM Optical Add/Drop Multiplexing (1551/1571/1591/1611nm) Physical Interface Card (PIC)	●	●	●	●	●	●	●	●
CR2D00 EEGF11	20-Port 100/1000Base-X-CSFP Physical Interface Card (PIC)	-	-	-	-	●	●	●	●
CR2D0E AGFE10	10-Port 100/1000Base-X-SFP Physical Interface Card E (PIC-E)	-	-	-	-	●	●	●	●
CR2D0L 2XFE10	2-Port 10GBase LAN/WAN-SFP+ Physical Interface Card E (PIC-E)	-	-	-	-	●	●	●	●
CR5D00 AUXQ10	Auxiliary Flexible Interface Card with 4-Port 100Base-RJ45 (FIC, Supporting 1588v2)	●	●	●	●	●	●	●	●
CR2D00 MPAA90	4-Channel FXS/FX0+2-Channel E&M+2-Channel RS232+2-Channel RS485 Board	●	●	●	●	●	●	-	-
CR2D00 MP8A90	4 Channels C37.94 Optical Interface and 4 Channels CoDir64K Electric Interface Board	●	●	●	●	●	●	-	-
CR2D00 OSA890	8-Channel V. 35/X. 21/V. 24 Board	●	●	●	●	●	●	-	-
CR2D0E 5XMF10	2-Port 50GBase/1-Port 100GBase-QSFP28 Physical	-	-	-	-	-	-	●	●

Model	Description	NSP -50	NSP- 50-E	NSP -12 0	NSP-1 20-E	NS P- A	NS P- B	NS P- C	NS P- D
	Interface Card(PIC)								
CR2D00 E2NF10	2-Port 100GBase-QSFP28 Physical Interface Card(PIC)	-	-	-	-	-	-	-	●
CR2D00 E1NC11	1-Port 100GBase-CFP2Physical Interface Card(PIC)	-	-	-	-	-	-	●	●
CR2D00 LAXF11	10-Port 10GBase LAN/WAN-SFP+ Physical Interface Card(PIC)	-	-	-	-	-	-	●	●
CR5D00 E4XF20	4-Port 10GBase-SFP+MACsec Interface Card	-	-	-	-	●	●	-	●
CR5D00 E1NB20	1-Port 100GBase-QSFP28+MACsec Interface Card	-	-	-	-	-	-	-	●
CR5DE2 NE4X10	2-Port 100GBase-QSFP28/1-Port100 GBase-QSFP28+4-Port 10GBase-SFP+MACsec Interface Card	-	-	-	-	-	-	-	●
CR2D0E M4TP10	4 Channels GE/FE PoE Electrical Interface Board	●	●	●	●	●	●	●	●
CR2D00 OEM890	6 Channels E&M Interface Board	●	●	●	●	●	●	●	●
CR2D00 ODE110	16-Port E1 Physical Interface Card(PIC, 75ohm) ,High anti-corrosion	●	●	●	●	●	●	●	●

**Table 3** List of subcards on the NSP

The following boards will be covered during this evaluation (● means related):

Module	Description	NE08E-S6E

Module	Description	NE08E-S6E
NEDD00CXPA00	System Control, Cross-connect and Multi-protocol Process Unit A	●
NEDD00CXPB00	System Control, Cross-connect and Multi-protocol Process Unit with 160G	●
NEJD00CXPA00	System Control, Cross-connect and Multi-protocol Process Unit	—
NEKD00EX4S00	4 Channels 10GE Optical Interface Board(SFP+)	●
NEDD00EX2S00	2 Channel 10GE Optical Interface Board(SFP+)	●
NEDD000EX1S0	1 Channel 10GE Optical Interface Board(SFP+)	●
NEDD00EM8F01	8 Channels GE/FE Optical Interface Board	●
NEDD00EM4F01	4 Channels GE/FE Optical Interface Board	●
NEDD00EM4T01	4 Channels GE/FE Electrical Interface Board	●
NEDD00EM8T01	8 Channels GE/FE Electrical Interface Board	●
NEDD00CQ1B00	4 Channels Channelized OC-3c/STM-1c POS Optical Interface Board	●
NEDD16E17502	16 Channels E1 Interface Board(75ohm)	●
NEDD32E17501	32 Channels E1 Interface Board(75ohm)	●
NEDD16E11202	16 Channels E1 Interface Board(120ohm)	●
NEDD32E11201	32 Channels E1 Interface Board(120ohm)	●
NEDD01MPAA00	4-Channel FXS/FX0+2-Channel E&M+2-Channel RS232+2-Channel RS485 Board	●
NEDD001SA800	8-Channel V. 35/X. 21/V. 24 Board	●
NEDD01MP8A00	4 Channels C37.94 Optical Interface and 4 Channels CoDir64K Electric Interface Board	●
NEDD0EM4TP00	4 Channels GE/FE PoE Electrical Interface Board	●
NEDD001EM600	6 Channels E&M Interface Board	●
CR5D00E4XF20	4-Port 10GBase-SFP+MACsec Interface Card	●

**Table 4** List of boards of NE08E

### 1.4.3 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. Traffic Forwarding
4. Auditing
5. Communication Security
6. IP-based ACL
7. Security functionality management
8. Cryptographic functions
9. SNMP Trap

These features are described in more detail in the subsections below.

#### 1.4.3.1 Authentication

The TOE can authenticate administrative users by user name and password. VRP provides a local authentication scheme for this, or can optionally enforce authentication decisions obtained from a Radius or TACACS+ server in the IT environment.

Authentication is always enforced for virtual terminal sessions via SSH, and SFTP (Secured FTP).

#### 1.4.3.2 Access Control

The TOE controls access by levels. Four hierarchical access control levels are offered that can be assigned to individual user accounts:

User level	Level name	Purpose	Commands for access
0	Visit	Network diagnosis and establishment of remote connections.	ping, tracet, language-mode, super, quit, display
1	Monitoring	System maintenance and fault diagnosis.	Level 0 and display, debugging, reset, refresh, terminal, send
2	Configurat ion	Service configuration.	Level 0, 1 and all configuration commands.
3	Managem ent	System management (file system, user management,	All commands.

User level	Level name	Purpose	Commands for access
		internal parameters).	

**Table 5** Access Levels

To implement refined right management, the user can extend the command level range to levels 0 to 15. If the user does not adjust the level of any command, the levels of the registered commands are automatically adjusted as follows after the command level range is extended to levels 0 to 15:

- The user access level 0 maps to the command level 0
- The user access level 1 maps to the command level 1
- The user access level 2 maps to the command level 10.
- The user access level 3 maps to the command level 15.
- For the command levels 2 to 9 and 11 to 14, no command line exists. The user can add command lines to these command levels to implement refined right management.

The TOE can either decide the authorization level of a user based on its local database, or make use of Radius or TACACS+ servers to obtain the decision whether a specific user is granted a specific level.

### 1.4.3.3 Traffic Forwarding

The TOE handles forwarding policy at their core. The forwarding engine controls the flow of network packets by making (and enforcing) a decision with regard to the network interface that a packet gets forwarded to.

These decisions are made based on a routing table that is either maintained by administrators (static routing) or gets updated dynamically by the TOE when exchanging routing information with peer routers.

### 1.4.3.4 Auditing

VRP generates audit records for security-relevant management actions and stores the audit records in storage device 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.
- For security management purpose, the administrators can select which events are being audited by enabling auditing for individual modules (enabling audit record generation for related to functional areas), and by selecting a severity level. Based on the hard-coded association of audit records with modules and severity levels, this allows control over the types of audit events being recorded.
- Output logs to various channels such as monitor, log buffer, trap buffer, file.
- Review functionality is provided via the command line interface, which allows administrators to inspect the audit log.

### 1.4.3.5 Communication Security

The TOE provides communication security by implementing SSH protocol. SSH2 (SSH2.0) is implemented. SSH2 is used for all 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, by RSA or by password with RSA;
- AES encryption algorithms
- Secure cryptographic key exchange by DH-exchange-group-sha1, DH-group14-sha1
- HMAC-SHA256 is used as verification algorithm for SSH

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

STelnet and SFTP are provided to implement secure Telnet and FTP, as alternatives to Telnet and FTP which are deemed to have known security issues. The S-Telnet is implemented by SSH.

### 1.4.3.6 IP-based ACL

VRP offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces on Interface boards. Information flow that is processed with ACL and to be forwarded to other network interfaces is not within the scope of the evaluated configuration. Outgoing information flow processed with ACL towards other network interfaces is not 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 Interface boards 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, type and code of ICMP protocol, fragment flag, can be used for ACL rule configuration.

### 1.4.3.7 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:

- Setup to enable SSH
- Setup to enable authentication for BGP, OSPF, IS-IS, LDP
- Setup to enable audit, as well as suppression of repeated log records
- Setup to change default rate limit plan

### 1.4.3.8 Cryptographic functions

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

- Supports encryption algorithms, such as AES encryption, for SSH;
- RSA is used in user authentication when user tries to authenticate and gain access to the TOE;
- HMAC-SHA256 is used as verification algorithm for SSH;
- MD5 is used as verification algorithm for packets of OSPF, BGP, IS-IS and LDP protocols;

### 1.4.3.9 SNMP Trap

The Simple Network Management Protocol (SNMP) is a network management protocol widely used in the TCP/IP network. SNMP is a method of managing network elements through a network console workstation which runs network management software.

A trap is a type of message used to report an alert or important event about a managed device to the NM Station.

The TOE uses SNMP traps to notify a fault occurs or the system does not operate properly.

## 1.4.4 TSF and Non-TSF data

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

#### **TSF data:**

- User account data, including the following security attributes:
  - User identities.
  - Locally managed passwords.
  - Locally managed access levels.
- Audit configuration data.
- Audit records.
- Configuration data of security feature and functions
- Routing and other network forwarding-related tables, including the following security attributes:
  - Network layer routing tables.
  - Link layer address resolution tables.
  - BGP, OSPF and IS-IS databases.
- Network traffic destined to the TOE processed by security feature and functions.

#### **Non-TSF data:**

- Network traffic to be forwarded to other network interfaces.

- Network traffic destined to the TOE processed by non-security feature and functions.

## 2 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 TOE claims EAL2 augmented with ALC\_FLR.2.

No conformance to a Protection Profile is claimed.

### 3 TOE Security problem definition

#### 3.1 Threats

The assumed security threats are listed below.

The **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) 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 the following **Table**.

Threat Name	Threat Definition
T.UnwantedNetworkTraffic	Unwanted/malicious network traffic designated to the TOE or pass through the TOE jeopardizes the integrity or the availability of the TOE, causing: <ol style="list-style-type: none"> <li>1. Denial of service of the TOE and may further cause the TOE fails to respond to system control and security management operations</li> <li>2. the traffic flows to unauthorized destinations</li> </ol>
T.UnauthenticatedAccess	A user who is not a user of the TOE gains access to the TOE.
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. This threat also includes data leakage to non-intended person or device
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 LMT/RMT.

**Table 6** List of identified threats

#### 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 console interface used for initial configuration, access of storage device) is protected against unauthorized physical access.

### 3.2.1.2 Network Elements

#### A.NetworkElements

The environment is supposed to provide supporting mechanism to the TOE:

- Peer router(s) for the exchange of dynamic routing information;
- A remote entities (PCs) used for administration of the TOE.
- (optional) RADIUS/TACACS+ used to provide remote authentication
- (optional) NMS, logging server, and SNMP trap server used for administration of the TOE

These entities are considered trusted and will not attack the TOE.

The administrator shall ensure the session between the TOE and the RADIUS/TACACS+/Logging server is secured when these servers are used.

### 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 Interface boards in the TOE are accessible.

### 3.2.1.4 Personnel Assumptions

#### A.NOEVIL

The authorized 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.

## 4 Security Objectives

### 4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O. DeviceAvail** The TOE shall ensure its own availability.
- **O.UserAvail** The TOE shall ensure only authorized users can access network resources through the TOE.
- **O. DataFilter** The TOE shall ensure that only allowed traffic goes through the TOE.

- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.
- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- **O.Authentication** The TOE shall authenticate its users before the users can assess the TSF functions.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrator 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, and Radius and TACACS+ servers for obtaining authentication and authorization decisions. The operational environments shall provide secure communication for the RADIUS/TACACS+/Logging server if these servers are used.
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console, and storage device inserted in the MPU) shall be protected against unauthorized physical access.
- **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 Interface boards in TOE serving the application (or public) network.
- **OE. Person** Personnel working as authorized administrators 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.

Threat	Rationale for security objectives to remove threats
T.UnwantedTraffic	This threat is countered by O.DeviceAvail, ensuring the TOE remain available, O.UserAvail ensuring the network remains available and O.DataFilter ensuring that unwanted data is filtered and cannot access/jeopardize the network resources.
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 LMT/RMT and the TOE and SNMPv3 for communication between the TOE and the SNMP Trap Server. (O.Communication).

**Table 7** Mapping Objectives to Threats

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.

Environmental Objective	Assumption
OE.NetworkElements	A.NetworkElements
OE.Physical	A.PhysicalProtection
OE.NetworkSegregation	A.NetworkSegregation
OE. Person	A.NOEVIL

**Table 8** Mapping Objectives for the Environment to Assumptions

## **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.
- Iteration: indicated by adding a string starting with “/” (e.g. “FCS\_COP.1/AES”), or by appending the iteration number in parenthesis, e.g. (1), (2), (3).

### 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:

- 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:**
  - 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. **command level management**
    1. **add, delete, modify**
  - iv. **authentication policy modification**
  - v. **system management**
    1. **reset to factory settings**
  - vi. **log management**

### 1. log policy modification]

FAU\_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[interface (if applicable), workstation IP (if applicable), User ID (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 **[the users of user level 3 with command-privilege level 15]** 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\_SAR.3 Selectable audit review

FAU\_SAR.3.1 The TSF shall provide the ability to apply **[selection]** of audit data based on **[filename]**.

#### 6.2.1.5 FAU\_STG.1 Protected audit trail storage

FAU\_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU\_STG.1.2 The TSF shall be able to **[prevent]** unauthorised modifications to the stored audit records in the audit trail.

#### 6.2.1.6 FAU\_STG.3 Action in case of possible audit data loss

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

### 6.2.2 Cryptographic Support (FCS)

#### 6.2.2.1 FCS\_COP.1/AES Cryptographic operation

FCS\_COP.1.1 The TSF shall perform **[symmetric de- and encryption]** in accordance with a specified

cryptographic algorithm **[AES CTR Mode]** and cryptographic key sizes **[128bits, 256bits]** that meet the following: **[FIPS 197]**

#### **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 **[RSASSA-PKCS-v1\_5 with SHA1]** and cryptographic key sizes **[configured (2048bits)]** that meet the following: **[RSA Cryptography Standard (PKCS#1 v2.1 (RFC3447) )]**

#### **6.2.2.3 FCS\_COP.1/MD5 Cryptographic operation**

FCS\_COP.1.1 The TSF shall perform **[authentication]** in accordance with a specified cryptographic algorithm **[MD5]** and cryptographic key sizes **[none]** that meet the following: **[RFC 1321]**

#### **6.2.2.4 FCS\_COP.1/HMAC-SHA256 Cryptographic operation**

FCS\_COP.1.1 The TSF shall perform **[authentication]** in accordance with a specified cryptographic algorithm **[HMAC-SHA256]** and cryptographic key sizes **[256 bits]** that meet the following: **[RFC 2104]**

#### **6.2.2.5 FCS\_COP.1/DHKeyExchange Cryptographic operation**

FCS\_COP.1.1 The TSF shall perform **[Diffie-Hellman key agreement]** in accordance with a specified cryptographic algorithm **[diffie-hellman-group14-sha1 and diffie-hellman-group-exchange-sha1]** and cryptographic key sizes **[diffie-hellman-group14-sha1: 2048 bits, diffie-hellman-group-exchange-sha1: 1024bits to 8192bits]** that meet the following: **[RFC 4253/RFC4419]**

#### **6.2.2.6 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 **[SSH key derivation]** and specified cryptographic key sizes **[128bits, 256bits]** that meet the following:**[RFC 4253]**

#### **6.2.2.7 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 **[configured (2048bits)]** that

meet the following: **[RSA Cryptography Standard (PKCS#1)]**

#### **6.2.2.8 FCS\_CKM.1/HMAC\_SHA256 Cryptographic key generation**

FCS\_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SSH key derivation]** and specified cryptographic key sizes **[256 bits]** that meet the following:**[RFC 4253]**

#### **6.2.2.9 FCS\_CKM.1/DHKey Cryptographic key generation**

FCS\_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[DH Group Generation]** and specified cryptographic key sizes **[1024bits to 8192 bits]** that meet the following: **[RFC4419]**

#### **6.2.2.10 FCS\_CKM.4/AES Cryptographic key destruction**

FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[releasing memory so that it is eventually overwritten]** that meets the following: **[none]**

#### **6.2.2.11 FCS\_CKM.4/RSA Cryptographic key destruction**

FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwriting with 0]** that meets the following: **[none]**

#### **6.2.2.12 FCS\_CKM.4/HMAC\_SHA256 Cryptographic key destruction**

FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[Releasing Memory]** that meets the following: **[none]**

#### **6.2.2.13 FCS\_CKM.4/DHKey Cryptographic key destruction**

FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[Releasing Memory]** that meets 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 [ **access control policy**] on  
 [Subject: users;  
 Objects: commands /features provided by TOE;  
 Operation: Read access / write access /Deny access]

### 6.2.3.2 FDP\_ACF.1 Security attribute based access control

FDP\_ACF.1.1 The TSF shall enforce the [ **access control policy**] to objects based on the following:

[Subject security attributes

a) **users and their following security attributes:**

- user Identity
- user level assignment

Objects security attributes:

a) **commands and their following security attributes:**

- Commands and 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: [

- a) **Only authorized users are permitted access to commands and feature.**
- b) **Users can be configured with different user levels to control the device access permission.**
- c) **There are 4 user access levels numbered from 0-3 and 16 command levels numbered from 0 to 15, in ascending order of privileges.**
- d) **User access levels map to command levels according to**
  - **The user level 0 maps to the command level 0**
  - **The user level 1 maps to the command level 1**
  - **The user level 2 maps to the command level 10.**
  - **The user level 3 maps to the command level 15.**
  - **For the command levels 2 to 9 and 11 to 14, no command line exists. The user can add command lines to these command levels to implement refined right management.]**

FDP\_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

a) **the user has been granted authorization for the relevant level commands]**

FDP\_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following

additional rules: [

- a) the user has not been granted authorization for the commands targeted by the request, or
- b) the user is not granted authorization with a Command beyond user relevant level].

### 6.2.3.3 FDP\_DAU.1 Basic Data Authentication

FDP\_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [the authentication information of BGP, OSPF, SSH, SNMP, ISIS, LDP]

FDP\_DAU.1.2 The TSF shall provide [BGP, OSPF, SSH, SNMP, ISIS, LDP] with the ability to verify evidence of the validity of the indicated information.

### 6.2.3.4 FDP\_IFC.1(1) Subset information flow control- CPU-defend

FDP\_IFC.1.1(1) The TSF shall enforce [Control Plane Committed Access Rate (CPCAR)/Blacklist] on

[Subjects:

TOE interface through which traffic goes

Information:

Ingress Control Plane Traffic (all different types of packets can reach the control plane, such as routing protocol or exception packets (ip options), control traffic);

Operations:

Transmit Control Plane Traffic Flow;

Drop Control Plane Traffic Flow;

CAR(QoS) the Control Plane Traffic Flow;]

### 6.2.3.5 FDP\_IFC.1(2) Subset information flow control- Data plane traffic control

FDP\_IFC.1.1(2) The TSF shall enforce [ACLs] on

[Subjects:

TOE interface through which traffic goes

Information:

Traffic flows;

Operations:

Permit, Deny, CAR]

### 6.2.3.6 FDP\_IFF.1(1) Simple security attributes - CPU-defend

FDP\_IFF.1.1(1) The TSF shall enforce the **[Control Plane Committed Access Rate (CPCAR)/Blacklist]** based on the following types of subject and information security attributes[

**Subject: TOE logic CPU- interface through which traffic goes.**

**Subject security attributes:**

- ✓ **Configured Rate Limit per traffic type**
- ✓ **Packets per second permitted to control plane**
- ✓ **filtering traffic destined to CPU by blacklist**

**Information security attributes:**

- ✓ **Receive packets: Packets destined to device. such as OSPF.**
- ✓ **Packets which need further process: such as ARP miss packets.**
- ✓ **filtering traffic destined to CPU by blacklist]**

FDP\_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- ✓ **If the ingress Control Plane Traffic with security attributes that match the configured Control Plane packets type does not exceed the configured rate limits, the traffic is permitted to flow**
- ✓ **If the ingress Control Plane Traffic with security attributes that match the configured Control Plane packets type exceed the configured rate limits, the traffic is not permitted to flow and will be dropped.]**

FDP\_IFF.1.3(1) The TSF shall enforce the **[traffic statistic]**.

FDP\_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: **[none]**

FDP\_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:**[none]**

### 6.2.3.7 FDP\_IFF.1(2) Simple security attributes – Data plane traffic control

FDP\_IFF.1.1(2) The TSF shall enforce the **[ACLs]** 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(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[Network traffic is match TOE according to administratively configured policies**

**The specific information flow control rules associated with each policy are as follows:**

**ACL**

**Ingress or egress IP traffic with security attributes that match configured ACL policy rule will be processed according to that rule.]**

FDP\_IFF.1.3(2) The TSF shall enforce the **[none]**.

FDP\_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: **[none]**

FDP\_IFF.1.5(2) 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 ]** unsuccessful authentication attempts occur (since the last successful authentication of the indicated user identity) 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]**.

### 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:

- [
- a) **user ID**
- b) **user level**
- c) **password]**

### 6.2.4.3 FIA\_SOS.1 Verification of secrets

FIA\_SOS.1.1/a The TSF shall provide a mechanism to verify that secrets meet **[for text string used as seeds for MD5 authentication for OSPF, they are case sensitive and contain no whitespace, no question mark. A cipher text mode should be used and the length of text string should be 32 to 392 characters]**

FIA\_SOS.1.1/b The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for MD5 authentication for BGP, they are case sensitive and contain no whitespace, no question mark. A cipher password mode should be used and the length of password should be 32 to 392 characters]**

FIA\_SOS.1.1/c The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for MD5 authentication for ISIS, they are case sensitive and contain no whitespace, no question mark. A cipher password mode should be used and the length of password should be 32 to 392 characters]**

FIA\_SOS.1.1/d The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for MD5 authentication for LDP, they are case sensitive and contain no whitespace, no question mark. A cipher password mode should be used and the length of password should be 32 to 392 characters]**

FIA\_SOS.1.1/e The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for user authentication for SNMP and they are case sensitive. A cipher password mode should be used and the length of password should be at least 8 characters long]**

FIA\_SOS.1.1/f 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. A cipher password mode should be used and the length of password should be at least 8 characters long]**

Application Note: The password must contain at least eight characters; The password must consist of digits, upper- and lowercase letters, and special characters (not including spaces and question marks); The password cannot be the same as the user name, nor can it be the reverse of the user name; When a local administrator modifies its password, the new password cannot be the same as any of the previous 10 passwords

### 6.2.4.3 FIA\_UAU.1 Timing of authentication –Administrator 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.

### 6.2.4.6 FIA\_UAU.5 Multiple authentication mechanisms

FIA\_UAU.5.1 The TSF shall provide **[the following authentication mechanisms:**

- a) **Remote authentication (by RADIUS or TACACS+);**
- b) **Local Authentication by local database local of TOE]**

to support user authentication.

FIA\_UAU.5.2 The TSF shall authenticate any user's identity according to the following: [

- a) **For Remote authentication by RADIUS or TACACS+**
- b) **For local Authentication, the TSF will authenticate the administrator based on the configured Identification and Authentication scheme].**

### 6.2.4.7 FIA\_UID.1 Timing of identification – Administrator 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]** all the functions **[defined in FMT\_SMF.1]** to **[the administrator-defined roles].**

### 6.2.5.2 FMT\_MSA.1 Management of security attributes

FMT\_MSA.1.1/1 The TSF shall enforce the **[access control policy]** to restrict the ability to **[query, modify]** the security attributes **[identified in FDP\_ACF.1 and FIA\_ATD.1]** to the **[administrator-defined roles]**.

FMT\_MSA.1.1/2 The TSF shall enforce the **[Control Plane Committed Access Rate (CPCAR)/Blacklist]** to restrict the ability to **[query, modify, delete]** the security attributes **[identified in FDP\_IFF.1(1)]** to **[the roles which can match the Control Plane Committed Access Rate (CPCAR)/Blacklist and the policy action is permit]**.

FMT\_MSA.1.1/3 The TSF shall enforce the **[ACLs]** to restrict the ability to **[query, modify, delete]** the security attributes **[identified in FDP\_IFF.1(2)]** to **[the roles which can match the Control Plane Committed Access Rate (CPCAR)/Blacklist and the policy action is permit]**.

### 6.2.5.3 FMT\_MSA.3 Static attribute initialization

FMT\_MSA.3.1/1 The TSF shall enforce the **[access control policy]** to provide **[restrictive]** default values for security attributes **[Command Group associations]** that are used to enforce the SFP.

FMT\_MSA.3.1/2 The TSF shall enforce the **[Control Plane Committed Access Rate (CPCAR)/Blacklist]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT\_MSA.3.1/3 The TSF shall enforce the **[ACLs]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT\_MSA.3.2 The TSF shall allow **[administrator-defined roles]** to specify alternative initial values to override the default values when an object or information is created.

### 6.2.5.4 FMT\_SMF.1 Specification of Management Functions

FMT\_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- a) authentication, authorization, encryption<sup>1</sup> policy
- b) ACL policy
- c) user management
- d) definition of Managed Object Groups and Command Groups
- e) port security / cpcar]

### 6.2.5.5 FMT\_SMR.1 Security roles

FMT\_SMR.1.1 The TSF shall maintain the roles **[administrator-defined roles]** (refer to Table 5).

FMT\_SMR.1.2 The TSF shall be able to associate users with roles.

<sup>1</sup> The encryption policy dictates which cryptographic algorithm / key length is used in which situation

## 6.2.6 Protection of the TSF (FPT)

### 6.2.6.1 FPT\_STM.1 Reliable time stamps

FPT\_STM.1.1 The TSF shall be able to provide reliable time stamps.

## 6.2.7 TOE access (FTA)

### 6.2.7.1 FTA\_SSL.3 TSF-initiated termination

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

**SSH session will be terminated after a period which can be configured]**

### 6.2.7.2 FTA\_TSE.1 TOE session establishment

FTA\_TSE.1.1 The TSF shall be able to deny session establishment based on [

- a) **authentication failure**
- b) **Source IP address doesn't match IP address configured in ACL for user management.]**

## 6.2.8 Trusted Path/Channels (FTP)

### 6.2.8.1 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]**.

### 6.2.8.2 FTP\_ITC.1 Trusted channel

FTP\_ITC.1.1 The TSF shall provide a communication channel between itself and **(SNMP Trap Server)** 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 The TSF shall permit **[the TSF]** to initiate communication via the trusted channel.

FTP\_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[sending SNMP traps]**.

## 6.3 Security Functional Requirements Rationale

### 6.3.1 Security Requirements Dependency Rationale

Dependencies within the EAL2 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:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
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_SAR.3	FAU_SAR.1	FAU_SAR.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	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/AES Cryptographic key generation FCS_CKM.4/AES Cryptographic key destruction
FCS_COP.1/RSA Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/RSA Cryptographic key generation FCS_CKM.4/RSA Cryptographic key destruction
FCS_COP.1/MD5 Cryptographic operation	No Dependencies	MD5 uses no key, so the key generation is unnecessary here.
FCS_COP.1/HMAC-SHA256 Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/HMAC_SHA256 Cryptographic key generation FCS_CKM.4/HMAC_SHA256 Cryptographic key destruction
FCS_COP.1/DHKeyExchange Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DHKey Cryptographic key generation FCS_CKM.4/DHKey Cryptographic key destruction
FCS_CKM.1/AES Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/AES Cryptographic operation FCS_CKM.4/AES Cryptographic key destruction
FCS_CKM.1/RSA Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4 FCS_CKM.4	FCS_COP.1/RSA Cryptographic operation FCS_CKM.4/RSA Cryptographic key destruction

FCS_CKM.1/DHKey Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DHKeyExchange Cryptographic operation FCS_CKM.4/DHKey Cryptographic key destruction
FCS_CKM.1/HMAC_SHA256 Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/HMAC_SHA256 Cryptographic operation FCS_CKM.4/HMAC_SHA256 Cryptographic key destruction
FCS_CKM.4/RSA Cryptographic key destruction	FCS_CKM.1	FCS_CKM.1/RSA Cryptographic key generation
FCS_CKM.4/AES Cryptographic key destruction	FCS_CKM.1	FCS_CKM.1/AES Cryptographic key generation
FCS_CKM.4/DHKey Cryptographic key destruction	FCS_CKM.1	FCS_CKM.1/DHKey Cryptographic key generation
FCS_CKM.4/HMAC_SHA256 Cryptographic key destruction	FCS_CKM.1	FCS_CKM.1/HMAC_SHA256 Cryptographic key generation
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_DAU.1	No Dependencies	None
FDP_IFC.1(1)	FDP_IFF.1(1)	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1(2)	FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1(1) FMT_MSA.3	FDP_IFC.1(1) FMT_MSA.3
FDP_IFF.1(2)	FDP_IFC.1(2) FMT_MSA.3	FDP_IFC.1(2) FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No Dependencies	None
FIA_SOS.1	No Dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
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	[FDP_ACC.1 or FDP_IFC.1(1) FDP_IFC.1(2)] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FDP_IFC.1(1) FDP_IFC.1(2) FMT_SMR.1 FMT_SMF.1

FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_STM.1	No Dependencies	None
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_TRP.1	No Dependencies	None
FTP_ITC.1	No Dependencies	None

**Table 9 : Dependencies between TOE Security Functional Requirements**

### 6.3.2 Sufficiency and coverage

Objective	SFRs	Rationale
O.DeviceAvail O.UserAvail	FDP_IFC.1(1) FDP_IFF.1(1)	These SFRs apply CPCAR and Blacklist features to process packets sent to the CPU, ensuring device security and uninterrupted services when attacks occur.
	FDP_IFC.1(2) FDP_IFF.1(2)	These SFRs also apply ACL to limit both packets going to the Control/Management Plane and through the TOE further ensuring availability of TOE and network resources.
O.Communication	FTP_TRP.1	This SFR provides the secure communication between users and management interface of the TOE
	FTP_ITC.1	This SFR provides the secure communication between TOE and SNMP Trap Server
	FDP_DAU.1 FIA_SOS.1	These SFRs provide the secure communication between TOE and LMT/RMT and ensure that the secrets for this are long enough.
	FCS_COP.1/* FCS_CKM.1/* FCS_CKM.4/*	These SFRS provide the cryptographic services for the secure communication above.
O.DataFilter	FDP_DAU.1 FIA_SOS.1	These SFRs ensures only traffics from authenticated switches/routers can send to the TOE, and ensure that the secrets for this are long enough.
	FDP_IFC.1(2) FDP_IFF.1(2)	These SFRs apply ACL to limit both packets going to the Control/Management Plane and through the TOE and thereby ensure that only protected 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, either by local password or through RADIUS/TACACS servers.
	FTA_TSE.1 FIA_AFL.1 FTA_SSL.3 FIA_SOS.1	The SFRs support authentication by: <ul style="list-style-type: none"> <li>Refusing logins from certain IP addresses</li> <li>Not allowing unlimited login attempts</li> <li>Logging out users after an inactivity period</li> <li>Ensuring password quality</li> </ul>
O.Authorisation	FDP_ACC.1 FDP_ACF.1	These SFRs ensure that only properly authorized admins can access certain functions
	FMT_SMR.1 FIA_ATD.1	These SFRs defines authorization levels and ensure that upon login an administrator 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 FMT_MSA.3	These SFRs ensure that new admins only get limited access rights and specifies who can modify these access rights.
O.Audit	FAU_GEN.1, FAU_GEN.2 FPT_STM.1	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, FAU_SAR.3	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.

**Table 10 Objectives to SFR mapping rationale**

## 6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2+ components augmented with ALC\_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

## 6.5 Security Assurance Requirements Rationale

The evaluation assurance level 2+ augmented with ALC\_FLR.2, has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

# 7 TOE Summary Specification

## 7.1 TOE Security Functional Specification

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

### 7.1.1 Authentication

The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces. Detailed functions include:

- 1) Support authentication via local password. This function is achieved by comparing user information input with pre-defined user information stored in memory.
- 2) Support authentication via remote RADIUS/TACACS+ authentication server. This function is achieved by performing pass/fail action based on result from remote authentication server.
- 3) Support authenticate user login using SSH, by password authentication, RSA authentication, or combination. This function is achieved by performing authentication for SSH user based on method mentioned in 1).
- 4) 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.
- 5) Support max attempts due to authentication failure within certain period of

time(default 5 minutes - configurable). This function is achieved by providing counts on authentication failure.

- 6) Support limiting access by IP address. This function is achieved by comparing IP address of requesting session with configured value stored in memory.
- 7) Support for user individual attributes in order to achieve all the enumerated features: user ID, user level, and password.

(FCS\_COP.1/RSA, FDP\_DAU.1, 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),

## 7.1.2 Access Control

The TOE enforces an access control by supporting following functionalities:

- 1) Support 4 user access levels. This function is achieved by storing number as level in memory.
- 2) Support 16 command levels. This function is achieved by storing number as level in memory.
- 3) Support assigning access level to commands. This function is achieved by associating access level number with commands registered.
- 4) Support assigning access level to user ID. This function is achieved by associating access level number with user ID.
- 5) 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, FIA\_ATD.1, FDP\_ACF.1, FMT\_MOF.1, FMT\_MSA.1, FMT\_MSA.3, FMT\_SMF.1, FMT\_SMR.1)

## 7.1.3 Traffic Forwarding

The TOE forwards network traffic, enforcing decisions about the correct forwarding interface and assembling the outgoing network packets using correct MAC addresses:

- 1) Support ARP/BGP/OSPF/IS-IS /LDP protocol. This function is achieved by providing implementation of ARP/BGP/OSPF/IS-IS /LDP protocol.
- 2) Support routing information generation via OSPF protocol. This function is provided by implementation of OSPF protocol.
- 3) Support routing information generation via BGP protocol. This function is provided by implementation of BGP protocol.
- 4) Support routing information generation via IS-IS protocol. This function is provided by implementation of IS-IS protocol.
- 5) Support routing information generation via manual configuration. This function is achieved by storing static routes in memory.
- 6) Support LSP information generation via LDP configuration. This function is provided by implementation of LDP protocol.
- 7) Support importing BGP/static routing information for OSPF. This function is provided by implementation of OSPF protocol.
- 8) Support importing OSPF/static routing information for BGP. This function is

- provided by implementation of BGP protocol.
- 9) Support importing OSPF/static routing information for IS-IS. This function is provided by implementation of IS-IS protocol.
  - 10) BGP support cryptographic algorithm MD5. This function is achieved by performing verification for incoming BGP packets using MD5 algorithm.
  - 11) OSPF support cryptographic algorithm MD5. This function is achieved by performing verification for incoming OSPF packets using MD5 algorithm.
  - 12) IS-IS support cryptographic algorithm MD5. This function is achieved by performing verification for incoming IS-IS packets using MD5 algorithm.
  - 13) LDP support cryptographic algorithm MD5. This function is achieved by performing verification for incoming LDP packets using MD5 algorithm.
  - 14) Support disconnection session with neighbor network devices. This function is achieved by locating and cleaning session information.
  - 15) OSPF support routing information aggregation. This function is achieved by manipulating routes stored in memory.
  - 16) OSPF support routing information filtering. This function is achieved by manipulating routes stored in memory.
  - 17) IS-IS support routing information filtering. This function is achieved by manipulating routes stored in memory.
  - 18) Support ARP strict learning. This function is achieved by regulating ARP feature to accept entry generated by own ARP requests.
  - 19) Support IPv4 traffic forwarding via physical interface. This function is achieved by making routing decision based on routes generated by BGP/OSPF/IS-IS/static configuration.
  - 20) Support LSP traffic forwarding via physical interface. This function is achieved by making label decision based on routes generated by LDP configuration.
  - 21) Support sending network traffic to VRP for centralized processing where destination IP address is one of the interfaces' IP addresses of the TOE. This is achieved by checking whether the traffic's destination IP address is within the configured interfaces' IP addresses in the Interface boards in the TOE. If it is, the traffic will be sent to VRP in MPU for centralized processing.
  - 22) Supporting Traffic Statistics. This function is achieved by matching traffic by ACL and collecting statistics on the number of packets and bytes of matched traffic.  
(FDP\_IFC.1(2), FDP\_IFF.1(2), FIA\_SOS.1, FDP\_DAU.1)

#### 7.1.4 Auditing

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

- 1) Support classification based on severity level. This function is achieved where logging messages are encoded with severity level and output to log buffer.
- 2) Support enabling, disabling log output. This function is achieved by interpreting enable/disable commands and storing results in memory. Log output is performed based on this result.
- 3) Support redirecting logs to various output channels: monitor, log buffer, trap buffer, log file. This function is achieved by interpreting commands and storing results in memory or in log files in storage device. Log channel for output is selected prior to execution of redirecting.

- 4) Support log output screening, based on filename. This function is performed by providing filtering on output.
- 5) Support querying log buffer. This function is achieved by performing querying operation with conditions input.
- 6) Support cleaning log buffer. This function is achieved by cleaning log buffer in memory.
- 7) Support to automatically remove the oldest log file if the space of the storage device storing the log files is full.
- 8) Only the authorized administrators can monitor the logfile record, and operate the log files. The unauthorized users have no access to do those actions. And the actions of the authorized administrators will be logged.

(FAU\_GEN.1, FAU\_GEN.2, FPT\_STM.1, FAU\_SAR.1, FAU\_SAR.3, FAU\_STG.1, FAU\_STG.3)

### 7.1.5 Communication Security

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

- 1) Devices that can function as the S-Telnet client and server support SSHv2. Secure Telnet (S-Telnet) enables users to remotely and securely log in to the device, and provides the interactive configuration interface. The S-Telnet is implemented by SSH.
- 2) Support diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1 as key exchange algorithm of SSH. This function is achieved by providing implementation of diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1 algorithm.
- 3) Support AES encryption algorithm. This function is achieved by providing implementation of AES algorithm.
- 4) Support MD5 verification algorithm. This function is achieved by providing implementation of MD5 algorithm.
- 5) Support HMAC-SHA256 verification algorithm. This function is achieved by providing implementation of HMAC-SHA256 algorithm.
- 6) Support using different encryption algorithm for client-to-server encryption and server-to-client encryption. This function is achieved by interpreting related commands and storing the result in memory.
- 7) Support Secure-FTP. This function is achieved by providing implementation of Secure-FTP. SFTP is short for SSH FTP that is a secure FTP protocol
- 8) Support for RSA key construction and destruction by overwriting it with 0.  
(FCS\_COP.1/\*, FCS\_CKM.1/\*, FCS\_CKM.4/\*, FMT\_SMF.1, FDP\_DAU.1)
- 8) Support for AES/HMAC\_SHA256/DHKey construction and destruction by Releasing Memory.  
(FCS\_COP.1/\*, FCS\_CKM.1/\*, FCS\_CKM.4/\*)

### 7.1.6 ACL

TOE use ACL to deny unwanted network traffic to pass through itself.

IP-based ACL is provided for this situation to identify traffic flow by matching all or

part of IP source address, IP destination address, IP protocol number, TCP/UDP source port number, TCP/UDP destination, and port number, then to proceed with certain actions like rate limit, prioritization or discard.

(FDP\_IFC.1(2), FDP\_IFF.1(2))

## 7.1.7 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.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling of SSH for the communication between management workstation 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 management workstation.

Detailed function specification include following:

- 1) Support remotely managing the TOE using SSH.
- 2) Support enabling, disabling S-FTP;
- 3) Support configuration on service port for SSH;
- 4) Support configuration on RSA key for SSH;
- 5) Support configuration on authentication type, encryption algorithm for SSH;
- 6) Support authenticate user logged in using SSH, by password authentication, RSA authentication;
- 7) Support configuration on logout when no operation is performed on the user session within a given interval;
- 8) Support configuration on max attempts due to authentication failure within certain period of time(default 5 minutes - configurable);
- 9) Support configuration on limiting access by IP address;
- 10) Support configuration on commands' access level;
- 11) Support management on OSPF by enabling, disabling OSPF;
- 12) Support configuration on area, IP address range, authentication type of OSPF;
- 13) Support management on BGP by enabling, disabling BGP;
- 14) Support configuration on peer address, authentication type of BGP;
- 15) Support management on ISIS by enabling, disabling ISIS;
- 16) Support configuration on peer address, authentication type of ISIS;
- 17) Support management on LDP by enabling, disabling LDP;
- 18) Support configuration on peer address, authentication type of LDP;
- 19) Support management on ARP by specifying static ARP entry, aging time and frequency of dynamical ARP entry. This function is achieved by interpreting commands input and storing value in memory.
- 20) Support management on log by enabling, disabling log output;
- 21) Support configuration on log output channel, output host;

- 22) Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
  - 23) Support enabling, disabling SNMP Agent and Trap message sending function;
  - 24) Support enabling, disabling the switch to Send an Alarm Message of a Specified Feature to the NM Station ;
  - 25) Support setting the Source Interface, Queue Length and Lifetime of Trap message;
- Above functions are achieved by providing interpreting input commands and storing result of interpreting in memory. Some results like routes generated, ACLs will be downloaded into hardware to assist forwarding and other TSF functions.
- (FMT\_SMF.1)

### 7.1.8 Denial-of-Service Protection

The TOE uses three specific mechanisms to prevent Denial of Service against itself or the network it protects:

- CPCAR** (Control Plane Committed Access Rate) limits the rate of protocol packets sent to the control plane and schedules the packets to protect the control plane. The switch identifies service packets based on ACLs and applies the default CAR value to protocol packets so that a limited number of protocol packets are sent to the control plane. Security of the control plane is ensured. CPCAR can be used to set the rate at which classes of packets are sent to the CPU, or the total rate of packets sent to the CPU. When the rate exceeds the upper limit, the system discards excess packets to prevent CPU overload
- TCP/IP Attack Defense** Defense against TCP/IP attacks protects the CPU of the router against malformed packets, fragmented packets, TCP SYN packets, and UDP packets, ensuring that normal services can be processed.
- Application Layer Association** There are various application protocols on the router, but not all of them are used in actual networking. To save CPU resources and defend against attacks, unnecessary application protocol packets are not sent to the CPU for processing.

To save the resources of the router, you can apply application layer association. In this case, if a protocol is enabled, the protocol packets are sent; if a protocol is disabled, the protocol packets are discarded.

When application layer association is enabled, if the upper layer protocol is enabled, packets are sent to the CPU based on the configured bandwidth; if the upper layer protocol is disabled, packets are sent to the CPU at the lowest rate or are discarded. When application layer association is disabled, packets are sent to the CPU based on the configured bandwidth, regardless of whether the upper layer protocol is enabled.

(FDP\_IFC.1(1), FDP\_IFF.1(1))

### 7.1.9 Cryptographic functions

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

- 1) Support AES /RSA algorithms. This is achieved by providing implementations of AES /RSA algorithms.

- 2) Support MD5/HMAC-SHA256 algorithms. This is achieved by providing implementations of MD5/HMAC-SHA256 algorithms.
- 3) Support for RSA key construction and destruction overwriting it with 0 (FCS\_COP.1/\*, FCS\_CKM.1/\*, FCS\_CKM.4/\*)
- 4) Support for AES/HMAC\_SHA256/DHKey construction and destruction by Releasing Memory
- 5) Support diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1 as key exchange algorithm of SSH

### **7.1.10 Time**

The TOE supports its own clock, to support logging and timed log-outs. (FPT\_STM.1, FTA\_SSL.3)

### **7.1.11 SNMP Trap**

The TOE uses SNMP traps to notify a fault occurs or the system does not operate properly.

- 1) Support management on trap by enabling, disabling trap output;
- 2) Support configuration on trap output interface, output host;
- 3) Support configuration on trap based on fault categories, fault functionality, or modules where the faults occur.
- 4) Support SNMPv3 which provides:
  - a) Encrypted communication using AES algorithm.
  - b) Packet authentication using SHA algorithms

(FTP\_ITC.1, FDP\_DAU.1)

## 8 Abbreviations, Terminology and References

### 8.1 Abbreviations

CC	Common Criteria
CLI	Command Line Interface
IS-IS	Intermediate System to Intermediate System
LMT	Local Maintenance Terminal
LPU	Line Process Unit
NE	NetEngine
NMS	Network Management System
NSP	Network Service Processor
OFC	Optical Flexible Card
PIC	Physical Interface Card
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFE	Switch Fabric Extend unit
SFR	Security Functional Requirement
SFU	Switch Fabric Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
MD5	Message-Digest Algorithm 5
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman

## 8.2 Terminology

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

*Administrator:* An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE’s point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

*Operator* See User.

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

## 8.3 References

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

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