# Huawei NetEngine5000E Core Router V800R006 Security Target

Version: 1.6

Last Update: 2014-08-28

Author: Huawei Technologies Co., Ltd.

# Revision record

| Date | Revision Version | Change Description | Author |
|---|---|---|---|
| 2014-03-14 | 1.0 | revision for 5000E | Wangbo |
| 2014-4-18 | 1.1 | Update according to EORs<br>Update for Table 1 | Wangbo |
| 2014-5-16 | 1.3 | Update according to EORs found by bill | Wangbo |
| 2014-05-21 | 1.4 | Update according to EORs | Wangbo |
| 2014-06-05 | 1.5 | Update guidance | Wangbo |
| 2014-08-28 | 1.6 | Revise for final release | Wangbo |
| | | | |
| | | | |

# Table of Contents

# 1 Introduction

This Security Target is for the evaluation of Huawei NetEngine5000E Core Router V800R006.

## 1.1 Security Target Identification

| | |
|---|---|
| Name: | Huawei NetEngine5000E Core Router V800R006 Security Target |
| Version: | 1.6 |
| Build number | C00SPC200 |
| Publication Date: | 2014-08-28 |
| Author: | Huawei Technologies Co., Ltd. |

## 1.2 TOE Identification

| | |
|---|---|
| Name: | Huawei NetEngine5000E Core Router |
| Version: | V800R006 build C00SPC200 |

There are three types of chassis of an NE5000E single-system chassis as shown in **Error! Reference source not found.**. These chassis can also be used as Cluster Line-card Chassis (CLC) in NE5000E cluster systems. Besides the CLCs, there are Cluster Central Chassis (CCC) chassis in NE5000E cluster systems as shown in **Error! Reference source not found.**. CCCs are used to interconnect CLCs. NE5000E Core Routers also work in cluster mode with the configurations shown in **Error! Reference source not found.**.

| |
|---|
| Chassis: NE5000E-16<br>VRP software Version 8 Release 8 with the following identifier (VRPV800R008C00).<br>Forwarding Engine software Version 8 Release 6 with the following identifier (V800R006C00). |
| Chassis: NE5000E-X16<br>VRP software Version 8 Release 8 with the following identifier (VRPV800R008C00).<br>Forwarding Engine software Version 8 Release 6 with the following identifier (V800R006C00). |
| Chassis: NE5000E-X16A<br>VRP software Version 8 Release 8 with the following identifier (VRPV800R008C00).<br>Forwarding Engine software Version 8 Release 6 with the following identifier (V800R006C00). |
| Chassis: NE5000E-X16B<br>VRP software Version 8 Release 8 with the following identifier (VRPV800R008C00).<br>Forwarding Engine software Version 8 Release 6 with the following identifier (V800R006C00). |

**Table 1** Types of chassis used in NE5000E single-chassis systems

| |
|---|
| Chassis: NE5000E CCC |

| |
|---|
| VRP software Version 8 Release 8 with the following identifier (VRPV800R008C00).<br>Forwarding Engine software Version 8 Release 6 with the following identifier (V008R006C00). |
| Chassis: NE5000E CCC-A<br>VRP software Version 8 Release 8 with the following identifier (VRPV800R008C00).<br>Forwarding Engine software Version 8 Release 6 with the following identifier (V800R006C00). |

**Table 2** Types of CCC chassis used in NE5000E cluster systems

| |
|---|
| Cluster: CCC-0<br>This cluster consists of two CLCs.<br>The CLCs can be both NE5000E-16s, both NE5000E-X16s, both NE5000E-X16As, or a combination of any two of them. |
| Cluster: CCC-1<br>This cluster consists of one NE5000E CCC or one NE5000E CCC-A and a maximum of four CLCs.<br>The CLCs can be all NE5000E-16s, all NE5000E-X16s, all NE5000E-X16As, or a combination of NE5000Es, NE5000E-X16s, and NE5000E-X16As. |
| Cluster: CCC-2<br>This cluster consists of two NE5000E CCCs or two NE5000E CCC-As and a maximum of eight CLCs.<br>The CLCs can be all NE5000Es, all NE5000E-X16s, all NE5000E-X16As, or a combination of NE5000Es, NE5000E-X16s, and NE5000E-X16As. |

**Table 3** NE5000E cluster systems

| | |
|---|---|
| Sponsor: | Huawei |
| Developer: | Huawei |
| Certification ID: | SERTIT-061 |
| Keywords: | Huawei, VRP, Versatile Routing Platform, Core Routers |

## 1.3 Target of Evaluation (TOE) Overview

Huawei NetEngine5000E Core Router V800R006, the TOE, which has large capacity and high performance, is developed to meet the requirement of carrier-class reliability. Based on the powerful versatile routing platform (VRP), the NE5000E provides strong switching capabilities, dense ports, and high reliability. NE5000Es mainly serve as super-core nodes on carriers' backbone networks, core nodes on metropolitan area networks (MANs), egresses in large-scale Internet data centers (IDCs), or core nodes on large-scale enterprise networks. NE5000E clusters are positioned as super-core nodes on backbone networks, supporting Layer 3 routing and Multiprotocol Label Switching (MPLS) forwarding. The TOE consists of both hardware and software.

At the core of each chassis is the Versatile Routing Platform (VRP), the software for managing and running the router’s networking functionality. 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 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 Line Processing Units (LPU) 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 and LPUs, there are other types of boards on TOE, such as Switch Fabric Unit (SFU), Switch Fabric Extend unit (SFE), ICU, ECU and OFC. Only MPU and LPU are 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 and RSVP
- Local PCs used by administrators to connect to the TOE for access of the command line interface either through TOE’s console interface or 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 LPU 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 NetEngine5000E Core Router V800R006 from a physical architectural view and a software architectural view.

#### 1.4.1.1 Physical Architecture

##### 1.4.1.1.1 Physical Architecture of NE5000E CLC

A CLC consists of the following systems:

- Power distribution system
- Heat dissipation system
- Network management sub-system
- Functional host system

Except the network management system (NMS), all the other 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 CLC consists of the system backplane, MPUs, LPUs, and SFUs as depicted in **Figure 1**.

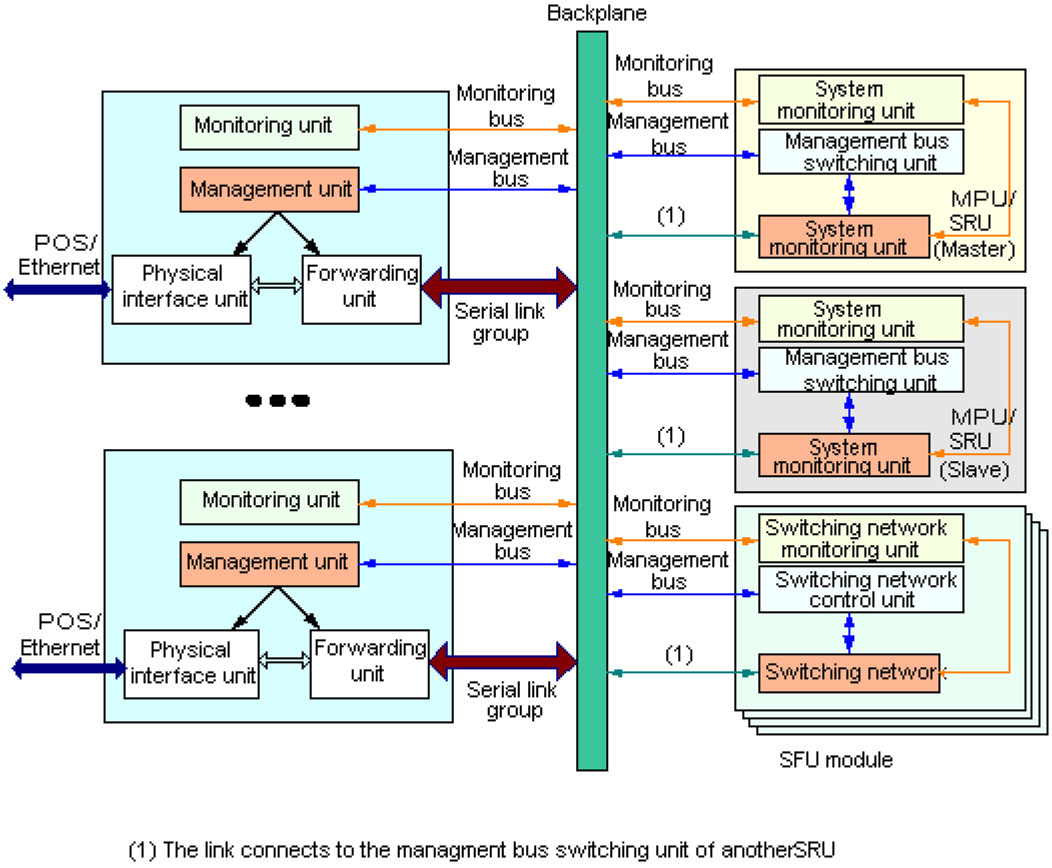

**Figure 1 Schematic diagram of the functional host system in a CLC**

#### 1.4.1.1.2 Physical Architecture of NE5000E CCC

A CCC consists of the following systems:

- Power distribution system
- Heat dissipation system
- Network management sub-system
- Functional host system

The functional host system consists of the system backplane, MPUs, optical flexible cards (OFCs), electrical cross units (ECUs), SFUs, and internal communication units (ICUs).The functional host system manages and controls the other systems, and provides control and data channels.

#### 1.4.1.1.4 Physical Architecture of NE5000E CCC-0 Cluster System

A CCC-0 system is the simplest NE5000E cluster. In a CCC-0 system, two CLCs (a master chassis and a slave chassis) are connected, as shown in **Figure 2**.

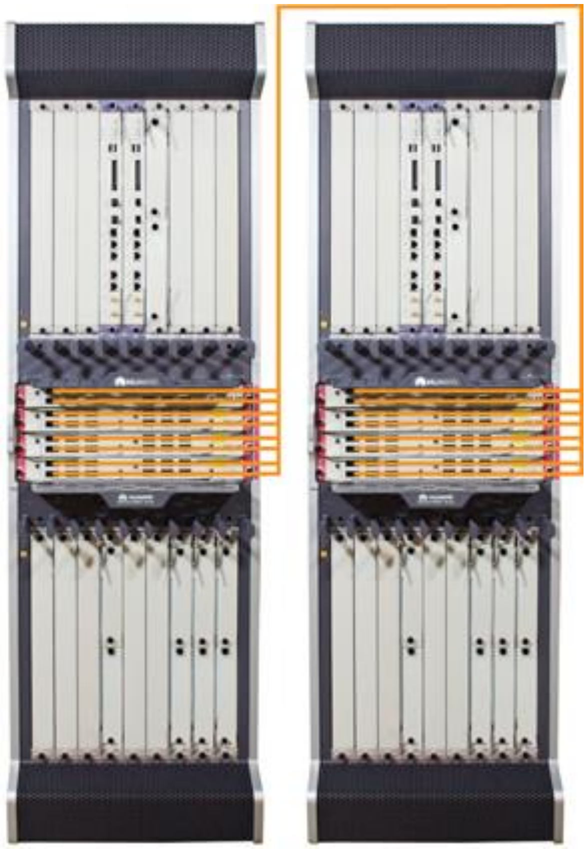

**Figure 2 Physical architecture of a CCC-0 system**

The physical architecture of a CCC-0 system is similar to that of a CLC, however, the functional host system of a CCC-0 system differs from that of a CLC and consists of two parts:

- Functional host system of the master chassis: processes data for both the master and slave chassis, and monitors and manages the power distribution systems and heat dissipation systems of both the master and slave chassis. The functional host system of the master chassis uses a network management interface to connect to the NMS.
- Functional host system of the slave chassis: manages the slave chassis.

In a CCC-0 cluster system, MPUs and LPUs in all chassis are within the scope of security evaluation.

#### 1.4.1.1.5 Physical Architecture of NE5000E CCC-1 Cluster System

A CCC-1 system consists of one CCC and a maximum of four CLCs, as shown in **Figure 3** and **Figure 4**.

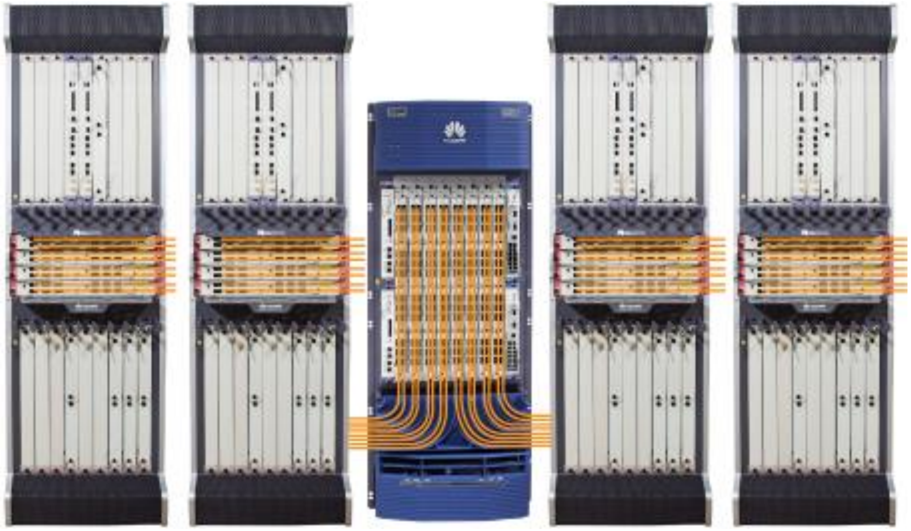

Figure 3 Physical architecture of a CCC-1 system (40G/100G cluster)

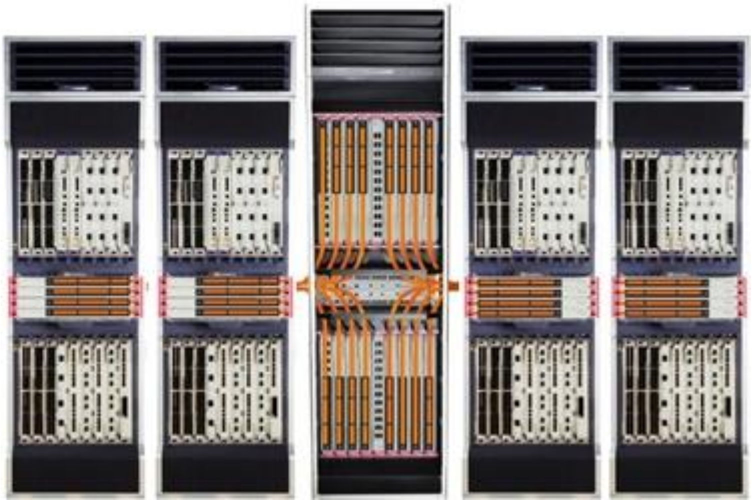

Figure 4 Physical architecture of a CCC-1 system (400G cluster)

A CCC-1 system uses stage-1, stage-2, and stage-3 switch fabrics. In a CCC-1 system, a CLC provides LPUs and stage-1 and stage-3 switch fabrics; a CCC provides a routing engine and a stage-2 switch fabric.

In a CCC-1 cluster system, MPUs and LPUs in all chassis are within the scope of security evaluation.

#### 1.4.1.1.6 Physical Architecture of NE5000E CCC-2 Cluster System

A CCC-2 system consists of two CCCs and a maximum of eight CLCs, as shown in **Figure 5** and **Figure 6**.

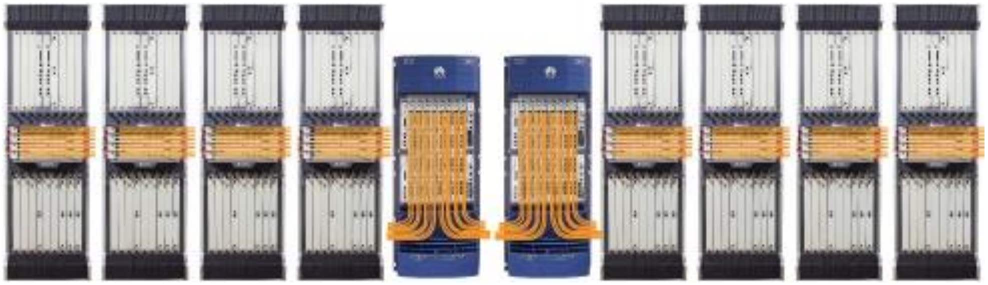

Figure 5 Physical architecture of a CCC-2 system (40G/100G cluster)

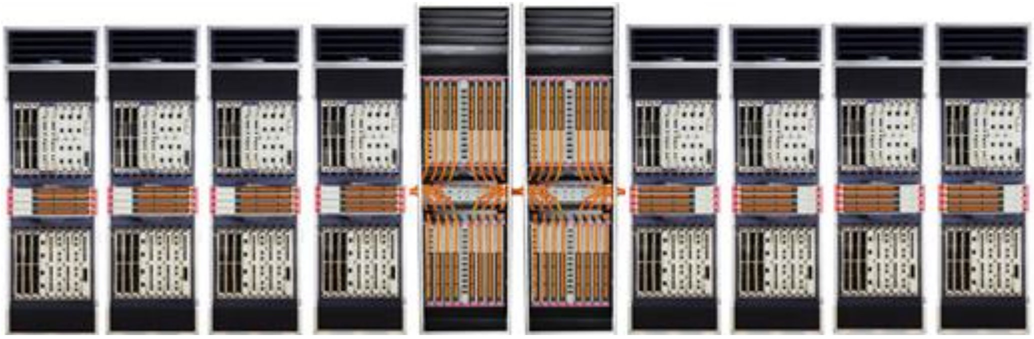

Figure 6 Physical architecture of a CCC-2 system (400G cluster)

A CCC-2 system uses stage-1, stage-2, and stage-3 switch fabrics. In a CCC-2 system, a CLC provides LPUs and stage-1 and stage-3 switch fabrics; a CCC provides a routing engine and a stage-2 switch fabric.

In a CCC-2 cluster system, MPUs and LPUs in all chassis are within the scope of security evaluation.

### 1.4.1.2 Software Architecture

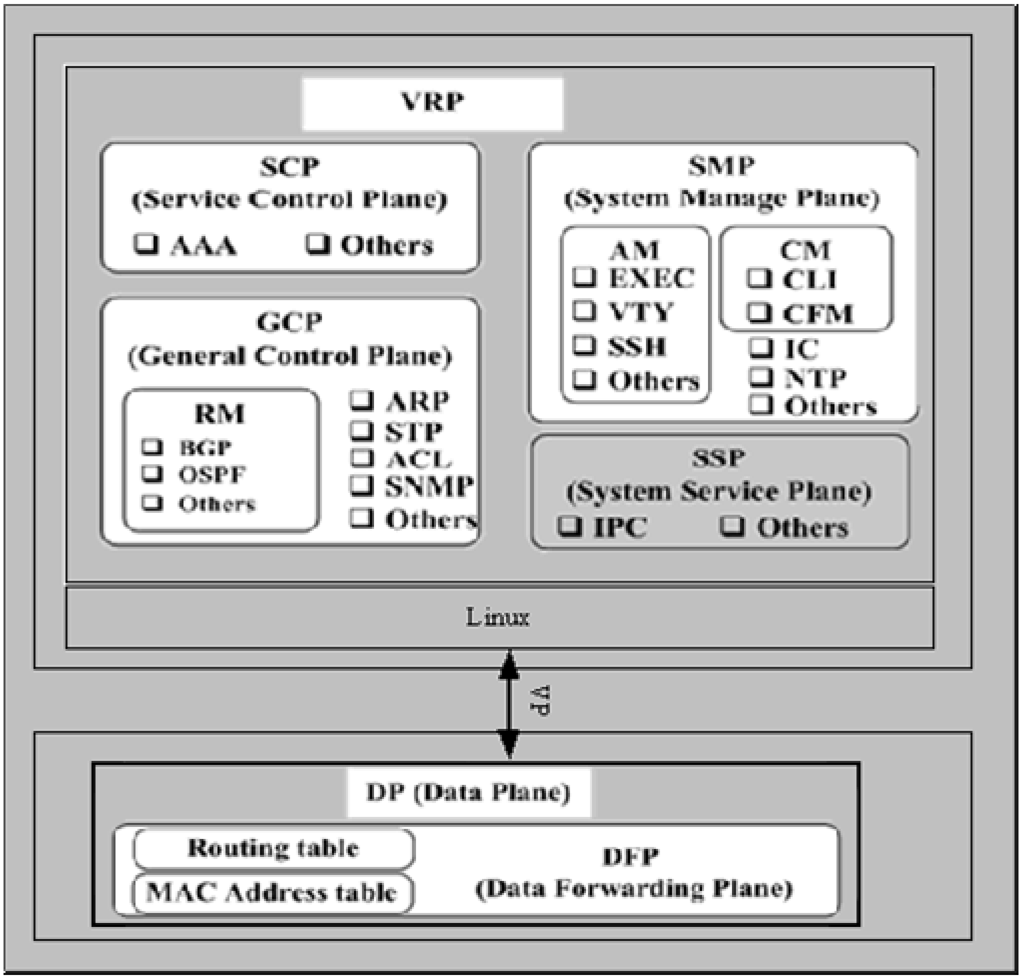

**Figure 7: TOE Software architecture**

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 LPU(s). The VRP includes Service Control Plane (SCP), System Management Plane (SMP), General Control Plane (GCP) and other TSF and non-TSF sub-systems.

**Figure 7** shows a brief illustration of the software architecture of the TOE.

### 1.4.2 Physical scope

This section will define the physical scope of the Huawei NetEngine5000E Core Router V800R006 to be evaluated.

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

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 four types of chassis of an NE5000E single-system chassis as shown in **Table 1**. These chassis can also be used as Cluster Line-card Chassis (CLC) in NE5000E cluster systems. Besides the CLCs, there are Cluster Central Chassis (CCC) chassis in NE5000E cluster systems as shown in **Table 2**. CCCs are used to interconnect CLCs. NE5000E Core Routers also work in cluster mode with the configurations shown in **Table 3**.

The following boards will be covered during this evaluation:

| Product Name | Board Name for Order | Description |
|---|---|---|
| NE5000E CLC | CR52K-BKPC-36U-8KW | NE5000E Integrated Chassis Components |
| | CR52-MPUB | Main Processing Unit B |
| | CR5DSFEBA06B | Switch Fabric Unit |
| NE5000E CCC | CR55C-BKPA/CR55C-BKPB | NE5000E Cluster Chassis |
| | CR5D0MPUA450 | Main Processing Unit A4 |
| | CR55C-MPUA | Main Processing Unit A |
| | CR5DSFUIA050 | Cluster 100G Central Switch Fabric Unit |
| | CR55C-ICUA | Cluster Internal Communication Unit A |
| | CR5DECUFA050 | Cluster 100G Electric Cross Unit |
| | CR5D00FCA060 | 100Gbps Cluster Optical Flexible Card |

| | | |
|---|---|---|
| NE5000E CCC-A | CR5D0MPUB550 | Main Processing Unit B550 |
| | CR5D00ICUB50 | Internal Communication Unit B50 |
| | CR5DSFUFK050 | Switch Fabric Unit |
| | CR5M00FCK050 | Optical Flexible Card |
| | CR5B0BKPCD50 | NE5000E-CCC-A Integrated Chassis Components DC |
| | CR5B0BKPCA50 | NE5000E-CCC-A Integrated Chassis Components DC |
| NE5000E-X16 | CR5B0BKP1660 | NE5000E-X16 Integrated Chassis Components |
| | CR5D0MPUB461 | Main Processing Unit |
| | CR5DSFUFA06B | 100G Switch Fabric Unit |
| | CR5D0SFUK06B | Switch Fabric Unit |
| NE5000E-X16A | CR5B0BKP166A | NE5000E-X16A Integrated Chassis Components DC |
| | CR5B0BKP166B | NE5000E-X16A Integrated Chassis Components AC |
| | CR5D0MPUB560 | Main Processing Unit B5 |
| | CR5DSFUFA06C | 100G Switch Fabric Unit C |
| | CR5DSFUIK06A | 400G Switch Fabric Unit A for Single Chassis |
| | CR5DSFUIK06B | 400G Switch Fabric Unit A for Cluster Chassis Access |
| NE5000E-X16B | CR5BBKP6BD60 | NE5000E-X16B Integrated Chassis Components DC |
| | CR5BBKP6BA60 | NE5000E-X16B Integrated Chassis Components AC |
| | CR5D0MPUB560 | Main Processing Unit B5 |
| | CR5DSFUIT060 | 1T Switch Fabric Unit A for Single Chassis |
| | CR5D00EFMB60 | 1T 24*40Gbps QSFP+ Interface Board |
| | CR5D00E8NC60 | 1T 8*100Gbps CFP2 Interface Board |

**Table 4** List of boards

| Type | Name | Version |
|---|---|---|
| Software | Product software | V800R006 |
| | VRP | Version 8 Release 8 |
| | Linux | Version: WRlinux4.1.0.0(CR5D0MPUA450, CR5D0MPUB550,CR5D0MPUB461, CR5D0MPUB560) /WRlinux3.0.3.0(CR52-MPUB, CR55C-MPUA) |
| Guidance | NE5000E V800R006C00 Product Manual | V1.0 |
| | Common Criteria Security Evaluation – Certified Configuration | V1.3 |

**Table 5** List of software and guidance

### 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). Authentication is always required for access via the console.

#### 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 | ping, tracert, |

| User level | Level name | Purpose | Commands for access |
|---|---|---|---|
| | | establishment of remote connections. | language-mode, super, quit, display |
| 1 | Monitoring | System maintenance and fault diagnosis. | Level 0 and display, debugging, reset, refresh, terminal, send |
| 2 | Configuration | Service configuration. | Level 0, 1 and all configuration commands. |
| 3 | Management | System management (file system, user management, internal parameters, …). | All commands. |

**Table 6** Access Levels

If no authentication for the console is configured, it operates at level 3.

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 levels of the original level-0 and level-1 commands remain unchanged.
- The level of the original level-2 commands is changed to level 10.
- The level of the original level-3 commands is changed to 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 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.

- 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, etc.
- 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. Two versions of SSH: SSH1 (SSH1.5) and SSH2 (SSH2.0) are implemented. But 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, by RSA/DSA or by password with RSA/DSA;
- 3DES/AES encryption algorithms
- Secure cryptographic key exchange by DH-exchange-group, DH-group1
- MD5 is used as optional HMAC 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.

#### 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 LPU. 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 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, type and code of ICMP protocol, fragment flag etc, 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, RSVP
- 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:

1) Supports encryption algorithms, such as 3DES-cbc, AES128/AES256 encryption, for SSH;
2) RSA and DSA are used in user authentication when user tries to authenticate and gain access to the TOE;
3) MD5 are used as option HMAC algorithm for OSPF, SSH and RSVP;
4) MD5 is used as verification algorithm for packets of 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 3.1R4.

The TOE claims EAL3+ augmented with ALC_CMC.4 (instead of ALC_CMC.3).

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, 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 7**.

| **Threat Name** | **Threat Definition** |
|---|---|
| T.UnwantedNetworkTraffic | Unwanted network traffic sent to the TOE will not only consume the TOE's processing capacity for incoming network traffic thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffic are sent to MPU from LPU within the TOE. This may cause denial of service of TOE.<br>This may further cause the TOE fails to respond to system control and security management operations.<br>Routing information exchanged between the TOE and peer routes may also be affected due to the traffic overload. |
| 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 7** 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 any console attached, access of CF card) 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:

- A Radius server or TACACS+ server for external authentication/authorization decisions;
- NMS, logging server and alarm server used for administration of the TOE

In addition, it is assumed the Radius server, and TACACS+ server, and the NMS are all trusted and will not be used to attack the TOE.

- 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 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 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 must authenticate users of its user access.
- **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.
- **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.
- **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 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 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).<br>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).<br>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 8** 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 9** 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.

## 6.2 TOE Security Functional Requirements

### 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 to 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].**

## Cryptography

### 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 CBC Mode]** and cryptographic key sizes **[128bits, 256bits]** that meet the following: **[FIPS 197]**

#### 6.2.2.2 FCS_COP.1/3DES Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[symmetric de- and encryption]** in accordance with a specified cryptographic algorithm **[3DES Outer CBC Mode]** and cryptographic key sizes **[168bits]** that meet the following: **[FIPS PUB46-3]**

#### 6.2.2.3 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 (512bits-2048bits)]** that meet the following: **[RSA Cryptography Standard (PKCS#1)]**

#### 6.2.2.4 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**

#### 6.2.2.5 FCS_COP.1/HMAC-MD5 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[authentication]** in accordance with a specified cryptographic algorithm **[HMAC-MD5]** and cryptographic key sizes **[16 bytes]** that meet the following: **[RFC 2104]**

#### 6.2.2.6 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-group1-sha1 and diffie-hellman-group-exchange-sha1]** and cryptographic key sizes **[diffie-hellman-group1-sha1: 1024 bits Oakley Group 2, diffie-hellman-group-exchange-sha1: 1024bits to 8192bits]** that meet the following: [**RFC 4253/RFC4419]**

#### 6.2.2.8 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 **[configured (512, 1024 & 2048bits)]** that meet the following: **[DSA Cryptography Standard (FIPS-186-3)]**

### 6.2.2.9 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]**

### 6.2.2.10 FCS_CKM.1/3DES 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 [**168bits]** that meet the following: **[RFC 4253]**

### 6.2.2.11 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 (512bits-2048bits)]** that meet the following: **[RSA Cryptography Standard (PKCS#1)]**

### 6.2.2.12 FCS_CKM.1/HMAC_MD5 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 **[16 bytes ]** that meet the following:**[RFC 4253]**

### 6.2.2.13 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]**

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 **[16 bytes]** that meet the following: **[RFC 4253]**

### 6.2.2.15 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 **[configured (512, 1024 &**

**2048bits)]** that meet the following: **[DSA Cryptography Standard (FIPS-186-3)]**

#### 6.2.2.16 FCS_CKM.4/3DES-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]**

#### 6.2.2.17 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]**

#### 6.2.2.18 FCS_CKM.4/HMAC_MD5 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy HMAC_MD5 keys in accordance with a specified cryptographic key destruction method **[Releasing Memory]** that meets the following: **[none]**

#### 6.2.2.19 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]**

#### 6.2.2.21 FCS_CKM.4/DSA 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]**

### 6.2.3 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 /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 **[VRP 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 16 user levels numbered from 0 to 15, in ascending order of priorities.**
d) **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 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, RSVP]**
FDP_DAU.1.2 The TSF shall provide **[BGP, OSPF, SSH, SNMP, ISIS, LDP, RSVP]** 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 .etc), control traffic);**

**Operations:**

**Transmit Control Plane Traffic Flow;**

**Drop Control Plane Traffic Flow;**

**CAR(QoS) the Control Plane Traffic Flo**w;]

### 6.2.3.5 FDP_IFC.1(2) Subset information flow control- Data plane traffic control

FDP_IFC.1.1(1) 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.etc**
- ✓ **Packets which need further process: such as ARP miss packets.etc**
- ✓ **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 (OSPF .etc.) 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 (OSPF .etc.) 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.etc.]**

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 HMAC-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 text string used as seeds for HMAC-MD5 authentication for RSVP, 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/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: All passwords must contain at least two normal characters, two capitals, 2 numbers and 2 special characters**.**

### 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 **[VRP 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 **[VRP information control policy (based on ACL)]** to restrict the ability *to **[query, modify, delete]*** the security attributes **[identified in FDP_IFF.1]** to **[the roles which can match the VRP information control policy (based on ACL) 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 **[VRP 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 **[VRP information control policy (based on ACL)]** 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[1] 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]** <u>(refer to table 6)</u>**.**

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

### 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)

[1] The encryption policy dictates which cryptographic algorithm / key length is used in which situation

#### 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 path between itself and (SNMP Trap Server) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated 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 require the use of the trusted path for **[sending SNMP traps]**.

## 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:

| Security Functional Requirement | Dependencies | Resolution |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 |
| FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.1 | FAU_GEN.1<br>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<br>Cryptographic operation | [FDP_ITC.1 or<br>FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1/AES<br>Cryptographic key generation<br>FCS_CKM.4/3DES-AES<br>Cryptographic key destruction |
| FCS_COP.1/3DES<br>Cryptographic operation | [FDP_ITC.1 or<br>FDP_ITC.2 or | FCS_CKM.1/3DES<br>Cryptographic key |

| | | |
|---|---|---|
| | FCS_CKM.1]<br>FCS_CKM.4 | generation<br>FCS_CKM.4/3DES-AES Cryptographic key destruction |
| FCS_COP.1/RSA Cryptographic operation | [FDP_ITC.1 or<br>FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1/RSA Cryptographic key generation<br>FCS_CKM.4/RSA Cryptographic key destruction |
| FCS_COP.1/HMAC-MD5 Cryptographic operation | [FDP_ITC.1 or<br>FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1/HMAC_MD5 Cryptographic key generation<br>FCS_CKM.4/HMAC_MD5 Cryptographic key destruction |
| FCS_COP.1/DHKeyExchange Cryptographic operation | [FDP_ITC.1 or<br>FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1/DHKey Cryptographic key generation<br>FCS_CKM.4//DHKey Cryptographic key destruction |
| | | |
| FCS_COP.1/DSA Cryptographic operation | [FDP_ITC.1 or<br>FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1/DSA Cryptographic key generation<br>FCS_CKM.4/DSA Cryptographic key destruction |
| FCS_CKM.1/AES Cryptographic key generation | [FCS_CKM.2, or<br>FCS_COP.1]<br>FCS_CKM.4 | FCS_COP.1/AES Cryptographic operation<br>FCS_CKM.4/3DES-AES Cryptographic key destruction |
| FCS_CKM.1/3DES Cryptographic key generationFCS_CKM.1 | [FCS_CKM.2, or<br>FCS_COP.1]<br>FCS_CKM.4FCS_COP.1 | FCS_COP.1/3DES Cryptographic operation<br>FCS_CKM.4/3DES-AES Cryptographic key destruction FCS_COP.1 |
| FCS_CKM.1/RSA Cryptographic key generationFCS_CKM.1 | [FCS_CKM.2, or<br>FCS_COP.1]<br>FCS_CKM.4FCS_CKM.4 | FCS_COP.1/RSA Cryptographic operationFCS_CKM.4<br>FCS_CKM.4/RSA Cryptographic key destruction |
| FCS_CKM.1/DHKey Cryptographic key generation | [FCS_CKM.2, or<br>FCS_COP.1]<br>FCS_CKM.4 | FCS_COP.1/DHKeyExchange Cryptographic operation<br>FCS_CKM.4/DHKey Cryptographic key |

| | | |
|---|---|---|
| | | destruction |
| FCS_CKM.1/HMAC_MD5 Cryptographic key generation | [FCS_CKM.2, or FCS_COP.1]<br>FCS_CKM.4 | FCS_COP.1/HMAC-MD5 Cryptographic operation<br>FCS_CKM.4/HMAC_MD5 Cryptographic key destruction |
| FCS_CKM.1/DSA Cryptographic key generation | [FCS_CKM.2, or FCS_COP.1]<br>FCS_CKM.4 | FCS_COP.1/DSA Cryptographic operation<br>FCS_CKM.4/DSA Cryptographic key destruction |
| | | |
| FCS_CKM.4/RSA Cryptographic key destruction | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1/RSA Cryptographic key generation |
| FCS_CKM.4/3DES-AES Cryptographic key destruction FCS_CKM.4 | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1/3DES Cryptographic key generation<br>FCS_CKM.1/AES Cryptographic key generation |
| | | |
| FCS_CKM.4/DHKey Cryptographic key destruction | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1/DHKey Cryptographic key generation |
| FCS_CKM.4/HMAC_MD5 Cryptographic key destruction | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1/HMAC_MD5 Cryptographic key generation |
| FCS_CKM.4/DSA Cryptographic key destruction | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1/DSA Cryptographic key generation |
| FDP_ACC.1 | FDP_ACF.1 | FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | FDP_ACC.1<br>FMT_MSA.3 |
| FDP_DAU.1 | No Dependencies | None |
| FDP_IFC.1(1) | FDP_IFF.1 | FDP_IFF.1 |
| FDP_IFC.1(2) | FDP_IFF.1 | FDP_IFF.1 |
| FDP_IFF.1(1) | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1<br>FMT_MSA.3 |
| FDP_IFF.1(2) | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1<br>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<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_ACC.1<br>FDP_IFC.1(1)<br>FDP_IFC.1(2)<br>FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1<br>FMT_SMR.1 |
| FMT_SMF.1 | No Dependencies | None |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.1 |
| FTP_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 10 : Dependencies between TOE Security Functional Requirements**

### 6.3.2 Sufficiency and coverage

| Objective | SFRs | Rationale |
|---|---|---|
| O.DeviceAvail<br>O.UserAvail | FDP_IFC.1(1)<br>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)<br>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<br>FIA_SOS.1 | These SFRs provide the secure communication between TOE and other switches/routers and ensure that the secrets for this are long enough. |
| | FCS_COP.1/*<br>FCS_CKM.1/*<br>FCS_CKM.4/* | These SFRS provide the cryptographic services for the secure communication above. |
| O.DataFilter | FDP_IFC.1(2)<br>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<br>FIA_UAU.1<br>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<br>FIA_AFL.1<br>FTA_SSL.3 | The SFRs support authentication by:<br>• Refusing logins from certain IP addresses<br>• Not allowing unlimited login attempts<br>• Logging out users after an inactivity period<br>• Ensuring password quality |
| O.Authorisation | FDP_ACC.1<br>FDP_ACF.1 | These SFRs ensure that only properly authorized admins can access certain functions |
| | FMT_SMR.1<br>FIA_ATD.1 | These SFRs defines authorization levels and ensure that upon login an administrator gets the proper authorization level. |
| | FMT_MOF.1<br>FMT_SMF.1 | These SFR lists certain management functions and restricts them to the proper authorization level. |
| | FMT_MSA.1<br>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,<br>FAU_GEN.2<br>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,<br>FAU_SAR.3 | These SFRs ensure that the correct users can read the correct information from the audit records. |
| | FAU_STG.1,<br>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 11 Objectives to SFR mapping rationale**

## 6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components augmented with ALC_CMC.4 (instead of ALC_CMC.3), as specified in [CC] Part 3. No operations are applied to the assurance components.

## 6.5 Security Assurance Requirements Rationale

The evaluation assurance level 3 augmented with ALC_CMC.4 (instead of ALC_CMC.3), 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/TACAS+ 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, DSA、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. 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, FCS_COP.1/DSA, 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 16 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, 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/RSVP protocol. This function is achieved by providing implementation of ARP/BGP/OSPF/IS-IS /LDP/RSVP 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 LSP information generation via RSVP configuration. This function is provided by implementation of RSVP protocol.
8) Support importing BGP/static routing information for OSPF. This function is provided by implementation of OSPF protocol.
9) Support importing OSPF/static routing information for BGP. This function is provided by implementation of BGP protocol.
10) Support importing OSPF/static routing information for IS-IS. This function is provided by implementation of IS-IS protocol.

11) BGP support cryptographic algorithm MD5. This function is achieved by performing verification for incoming BGP packets using MD5 algorithm.
12) OSPF support cryptographic algorithm HMAC-MD5. This function is achieved by performing verification for incoming OSPF packets using HMAC-MD5 algorithm.
13) IS-IS support cryptographic algorithm MD5. This function is achieved by performing verification for incoming IS-IS packets using MD5 algorithm.
14) LDP support cryptographic algorithm MD5. This function is achieved by performing verification for incoming LDP packets using MD5 algorithm.
15) RSVP support cryptographic algorithm HMAC-MD5. This function is achieved by performing verification for incoming RSVP packets using HMAC-MD5 algorithm.
16) Support disconnection session with neighbor network devices. This function is achieved by locating and cleaning session information.
17) OSPF support routing information aggregation. This function is achieved by manipulating routes stored in memory.
18) OSPF support routing information filtering. This function is achieved by manipulating routes stored in memory.
19) IS-IS support routing information filtering. This function is achieved by manipulating routes stored in memory.
20) Support ARP strict learning. This function is achieved by regulating ARP feature to accept entry generated by own ARP requests.
21) 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.
22) Support LSP traffic forwarding via physical interface. This function is achieved by making label decision based on routes generated by LDP configuration.
23) 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 LPU in the TOE. If it is, the traffic will be sent to VRP in MPU for centralized processing.

(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 CF card. 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 oldest log files if audit files exceed the size of store device.

(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. Two versions of SSH: SSHv1 (SSH1.5) and SSHv2 (SSH2.0) are implemented. But SSH2 is recommended for most cases by providing more secure and effectiveness in terms of functionality and performance. SFTP provide secure file transfer functionality.

1) Support SSHv1 and SSHv2. This function is achieved by providing implementation of SSHv1 and SSHv2.
2) Support diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1 as key exchange algorithm of SSH. This function is achieved by providing implementation of diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1 algorithm.
3) Support 3DES, AES encryption algorithm. This function is achieved by providing implementation of 3DES, AES algorithm.
4) Support MD5 verification algorithm. This function is achieved by providing implementation of MD5 algorithm.
5) Support HMAC-MD5 verification algorithm. This function is achieved by providing implementation of HMAC-MD5 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.
8) Support for RSA/DSA key construction and destruction by overwriting it with 0.

(FCS_COP.1/*, FCS_CKM.1/*, FCS_CKM.4/*, FMT_SMF.1, FDP_DAU.1)

### 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 port number etc, 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, etc.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling of SSH for the communication between LMT 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 LMT GUI.

Detailed function specification include following:

1) Support Local configuration through console port. Parameters include console port baud rate, data bit, parity, etc;
2) Support configuration for authentication and authorization on user logging in via console port;
3) Support configuration for authentication mode and authorization mode on user logging in via console port;
4) Support remotely managing the TOE using SSH.
5) Support enabling, disabling S-FTP;
6) Support configuration on service port for SSH;
7) Support configuration on RSA/DSA key for SSH;
8) Support configuration on authentication type, encryption algorithm for SSH;
9) Support authenticate user logged in using SSH, by password authentication, RSA/DSA authentication, or combination of both;
10) Support configuration on logout when no operation is performed on the user session within a given interval;
11) Support configuration on max attempts due to authentication failure within certain period of time;
12) Support configuration on limiting access by IP address;
13) Support configuration on commands’ access level;
14) Support management on OSPF by enabling, disabling OSPF;
15) Support configuration on area, IP address range, authentication type of OSPF;
16) Support management on BGP by enabling, disabling BGP;
17) Support configuration on peer address, authentication type of BGP;
18) Support management on ISIS by enabling, disabling ISIS;
19) Support configuration on peer address, authentication type of ISIS;
20) Support management on LDP by enabling, disabling LDP;
21) Support configuration on peer address, authentication type of LDP;
22) Support management on RSVP by enabling, disabling RSVP;
23) Support configuration on peer address, authentication type of RSVP;
24) 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.
25) Support management on log by enabling, disabling log output;
26) Support configuration on log output channel, output host;
27) Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
28) Support enabling, disabling SNMP Agent and Trap message sending function;
29) Support enabling, disabling the switch to Send an Alarm Message of a Specified

Feature to the NM Station ;

30) 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 AES128/AES256/3DES/RSA/DSA algorithms. This is achieved by providing implementations of AES128/AES256/3DES/RSA/DSA algorithms.
2) Support MD5/HMAC-MD5 algorithms. This is achieved by providing implementations of MD5/HMAC-MD5 algorithms.
3) Support for RSA/DSA key construction and destruction overwriting it with 0

(FCS_COP.1/*, FCS_CKM.1/*, FCS_CKM.4/*)

### 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 DES，3DES, AES128, AES192, AES256 algorithm.
    b) Packet authentication using MD5 algorithms

(FTP_ITC.1, FDP_DAU.1)

# 8 Abbreviations, Terminology and References

## 8.1 Abbreviations

| | |
|---|---|
| CC | Common Criteria |
| CCC | Cluster Central Chassis |
| CLC | Cluster Line-card Chassis |
| CLI | Command Line Interface |
| GUI | Graphical User Interface |
| IS-IS | Intermediate System to Intermediate System |
| LMT | Local Maintenance Terminal |
| LPU | Line Process Unit |
| MPU | Main Process Unit |
| NE | NetEngine |
| NMS | Network Management Sub-system |
| OFC | Optical Flexible Card |
| PP | Protection Profile |
| RMT | Remote Maintenance Terminal |
| SFE | Switch Fabric Extend unit |
| SFR | Security Functional Requirement |
| SFU | Switch Fabric Unit |
| SFU | Switching Fabric Unit |
| SPU | Service Process 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 |
| DSA | Digital Signature Algorithm |

## 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 4, September 2012

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 4, September 2012