Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300 Security Target

Version: 1.20

Last Update: 2015-12-14

Author: Huawei Technologies Co., Ltd.

Revision record

Date	Revision Version	Change Description	Author
2013-10-30	0.10	Initial Draft	Yinbaoguo
2013-12-10	0.20	Update product information	Yinbaoguo
2014-02-28	0.30	Update product information	Yinbaoguo
2014-03-06	0.40	Update product information	Yinbaoguo
2014-03-26	0.50	Update TSF functions	Yinbaoguo
2014-05-07	0.60	Updated based on the OBSERVATION REPORT	Yinbaoguo
2014-05-27	0.70	Update SFR description	Yinbaoguo
2014-05-30	0.80	Update hardware description	Yinbaoguo
2014-06-16	0.90	Update Table 1-3Evaluated platforms brief description	Yinbaoguo
2014-07-21	1.00	Update TOE Environment	Yinbaoguo
2014-09-13	1.10	Update information for EE comments	Yinbaoguo
2014-11-14	1.11	Change the version information SPC200 to SPC300 and the Hash values of SPC200 to those of SPC300	Sunhong
2015-1-28	1.12	Add the P/N number to the TOE identification	Sunhong
2015-3-7	1.13	Update information for ATE review 2015/2/18	Huhui
2015-04-20	1.14	Update information for EE comments	Yinbaoguo
2015-07-18	1.15	Update information.	HuHui
2015-08-07	1.16	Update information.	HuHui
2015-9-6	1.17	Update information	HuHui
2015-10-30	1.18	Update information	HuHui
2015-11-11	1.19	Update information	HuHui
2015-12-14	1.20	Update information	HuHui

Contents

Tables

Figures

1 Introduction

1.1 Security Target Identification

Name: Huawei Eudemon8000E/USG9500 Series Firewall V300R001C01SPC300 Security Target

Version: 1.20

Publication Date: 2015-12-14

Author: Huawei Technologies Co., Ltd.

1.2 TOE Identification

TOE name:

Huawei Eudemon 8000E-X/USG9500 Series Firewall

TOE version:

V300R001C01SPC300B113

Table 1-1 Naming conventions

HW identifier		
Eudemon*8000*E-Xn	Eudemon	Firewall Brand
	*8000*E	Series Name
	Xn	Model Name
Secospace USG*bbbb*	Secospace USG	Firewall Brand
	bbbb	Model Name

SW identifier

V*xxx*R*yyy*C*aa*SPC*bbb* Bccc	V*xxx*	Version Number
	R*yyy*C*aa*	Release Number
	SPC*bbb*	Patch number
	Bccc	Build number

Table 1-2 Evaluated platforms

Series Id	Model Name	ESN
Eudemon 8000E-X/USG9500	Eudemon8000E-X3	210235G6QB10E5000001
	Eudemon8000E-X8	210235GQD10E5000009
	Eudemon8000E-X8	210235G6QDZ0C5000008
	Eudemon8000E-X16	2102351931P0B5000301
	USG9520	210235G7F6

Table 1-3 Evaluated platforms brief description

Series Id	HW identifier	Dimension	LPU/SPU Slot Quantity	SFU Slot Quantity	MPU Slot Quantity
Eudemon 8000E-X	Eudemon8000E-X3/ Secospace USG9520	DC chassis: 442 mm x 650 mm x 175 mm AC chassis: 442 mm x 650 mm x 220 mm	3	0	2
	Eudemon8000E-X8/ Secospace USG9560	442mm×650mm×620mm	8	1	2
	Eudemon8000E-X16/ Secospace USG9580	442mm×650mm×1420mm	16	4	2

Sponsor: Huawei

Developer: Huawei

Certification ID:

Keywords: Firewall, High Availability, Traffic Filter

Note:

The Eudemon and the Secospace are the same, but sold as different brands for different areas.

The software running on the Eudemon8000E-X3 (Secospace USG9520) is a little different with that on Eudemon8000E-X8 (Secospace USG9560) because of hardware differences, but the functions are the same.

The software running on Eudemon8000E-X8 (Secospace USG9560) and that on Eudemon8000E-X16 (Secospace USG9580) is the same.

External entities: LMT, RMT, Radius server, Network devices, ELog.

1.3 Product Overview

Huawei Eudemon8000E/USG9000 Series Firewall , is a hardware platform and software image integrated as a whole system. It is designed to provide firewall, IPv6, Virtual Private Network (VPN), Virtual Local Area Network (VLAN) and anti-spam protection etc. to provide protection on TCP/IP networks. It can protect computer networks from abuse. The series firewall resides between the network it is protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy (set of rules) defined by the Security Administrator. In addition to providing stateful application-level protection, the TOE delivers a full range of network-level services including; firewall, IPv6, VPN, VLAN and anti-spam protection etc.; using dedicated, easily managed platforms.

1.4 Target of Evaluation (TOE) Overview

Eudemon8000E/USG9000 Series Firewall V300R001C01SPC300B113, the TOE, provides high-end networking capacities for telecom and enterprise core networks. It consists of both hardware and software.

The TOE, provides these major security features, authentication, access control, traffic security forwarding, communication security, flow control policy, security functionality management, cryptographic functions, clock function.

1.4.1 TOE Type

The TOE is a firewall system composed of a hardware platform and a software running within the platform as a whole system.

1.4.2 TOE Security Functionality

1.4.2.1 Authentication

The TOE can authenticate administrative users by user name and password. Administration may either be performed locally using the Local Console CLI or remotely using the Network Web-Based GUI or Network CLI. The TOE 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 network remote sessions via SSH, and SFTP (Secured FTP), HTTPS (Web-Based GUI) sessions. Authentication for access via the console is always enabled.

The TOE will establish the session after successful authentication, and terminate the session after the users log out.

When the number of unsuccessful authentication attempts has been surpassed, the TOE terminates the session of the user and lock the user.

1.4.2.2 Access Control Policy

The TOE access control is performed by VRP and includes the following:

- Users can be configured with different user levels to control their device access. User levels are configured by an administrator.
- User levels are marked by numbers from 0 to 15, where 0 is low privilege and 15 is full privilege
- User levels map to command levels (groups of commands). A user can run only commands at the same or lower level.

Table 1-4 Access Levels

User level	Command level	Level name	Description
0	0	Visit	Commands at this level are diagnosis commands such as ping and trace commands and commands that are used to access a remote device such as Telnet clients.
1	1	Monitoring	Commands at this level are system maintenance commands such as most display commands.
2	2	Configuration	Commands at this level are used for service configuration including routing commands and commands at each network layer to provide network services to users.
3-15	3	Management	Commands at this level are system basic operation commands that support services, including file system, FTP, TFTP, configuration file switching commands, user management commands, command level configuration commands, system parameter configuration commands, and debugging commands.

Visit level command is the command with command level 0, and the other levels are similar.

Visit level user is the user with user level 0, and the other levels are similar.

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.

1.4.2.3 Traffic Security Forwarding

The TOE handles security and forwarding policy at their core. The forwarding engine controls the flow of network packets by making (and enforcing) a decision permit or deny the traffic, 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.

1.4.2.4 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 and by RSA;

- 3DES/AES encryption algorithms;
- Secure cryptographic key exchange.

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

STelnet are provided implementing secure Telnet and FTP, to substitute Telnet and FTP which are deemed to have known security issues.

Note:

- The connection between the TOE and the RADIUS/TACACS server has to be over an IPSec tunnel.

1.4.2.5 Flow Control Policy

The TOE provides a policy mechanism based on security rules and traffic engineering rules. For each policy item, aspects like packet source and destination addresses, in and out interfaces, security zones, and ports can be used as filters, and actions like allow, block or even traffic engineering processes can be assigned. Through such mechanism, we can define a policy and drop attacks for the TOE itself.

The TOE also offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow. 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 prioritize, rate-limit the information flow destined to TOE through interfaces on LPU by matching information contained in the headers of connection-oriented or connectionless IP packets against ACL rules specified. Source IP address, destination IP address, IP protocol number, source port number if TCP/UDP protocol, destination port number if TCP/UDP protocol, TCP flag if TCP protocol, type and code if ICMP protocol, fragment flag etc, can be used for ACL rule configuration.

1.4.2.6 Security Functionality Management

Security functionality management includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

More functionalities include:

- Setup to enable SSH
- Setup to change default rate limit plan

1.4.2.7 Cryptographic functions

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

- AES is used as default encryption algorithm for SSH;
- 3DES is used as optional encryption algorithm for SSH;
- RSA is used in user authentication when user tries to authenticate and gain access to the TOE;
- HMAC-SHA is used as verification algorithm for packets of SSH protocols.

1.4.3 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.
- 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.
- 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.

1.4.4 Non-TOE hardware and software

Table 1-5 Non-TOE hardware and software

Non-TOE hardware	Radius or TACACS+ server
	Peer router
	Local PC
	Remote PC
	Physical network
Non-TOE software	None

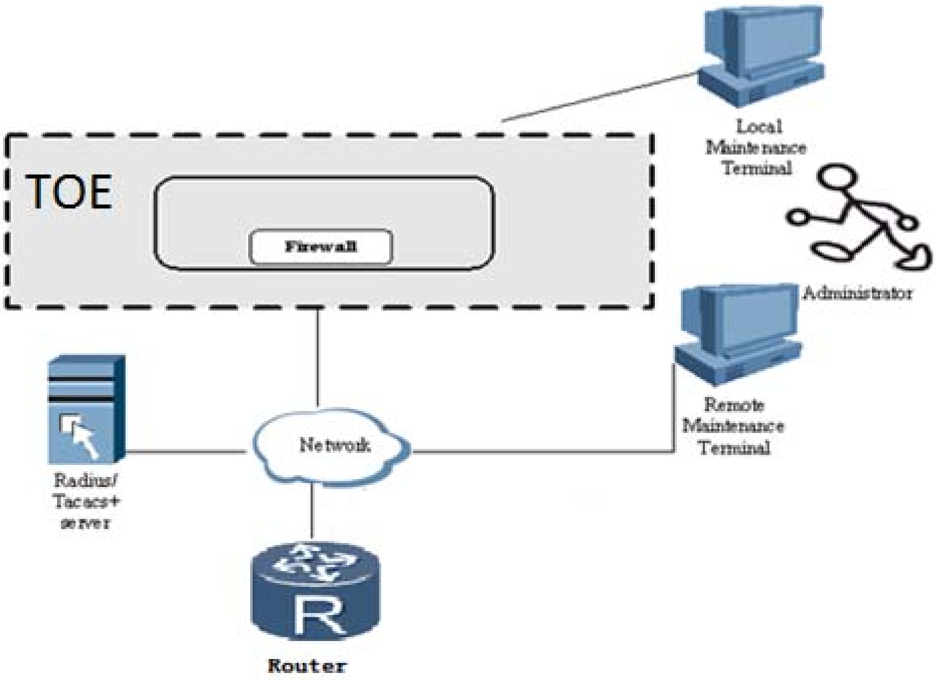


Figure 1-1 TOE boundary and IT environment

The environment for TOE comprises the following components:

- An optional Radius or TACACS+ server providing authentication and authorization decisions to the TOE (it must be compatible with L2TP[VPN], IPSEC[VPN] and x.509 certificates).
- Peer routers providing routing information to the TOE via dynamic protocols.
- Local PCs used by the administrators to connect to the TOE to access of the command line interface either through TOE's console interface or TOE's ETH interface. These connections are performed via a secure channel enforcing SSH. The SW within this PC is:
  - o Generic OS developed later than 2010 (Windows 7/8/8.1/10 or any Linux distribution)
  - o Generic Web browser developed later than 2014 with Javascript support.
  - o Generic SSH client with SSHv2 support
- Remote PCs used by the administrator to connect to the TOE to manage it. These connections are performed via a secure channel enforcing HTTP over SSL/TLS. It is required to install the https client on these PCs. The SW within this PC is:
  - o Generic OS developed later than 2010 (Windows 7/8/8.1/10 or any Linux distribution)
  - o Generic Web browser developed later than 2014 with Javascript support.
  - o Generic SSH client with SSHv2 support
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.

1.5 TOE Description

This section will introduce the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Boundary

1.5.1.1 Board Description

Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113, the TOE is a stateful firewall designed to provide DDOS, IPSec VPN, packet filtering etc. It offers a cost-effective system. It is a software security system designed to protect computer networks from abuse. In the following, we'll provide a detailed description of the board which is included in the TOE.

MPU/SRU: At the core of each firewall is the VRP deployed on board Main Processing Unit (MPU) or Switch Routing Unit (SRU), the software for managing and running the router's networking functionality. It provides extensive security features. These features include different interfaces with according access levels for administrators; enforcing authentications prior to establishment of administrative sessions with the TOE; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

LPU: The Line Processing Units (LPU) are the actual hardware providing network traffic processing capacity. Network traffic is hashed to SPU.

SPU: The Service Processing Units (SPU) are the actual hardware providing security processing capacity, For example, packet filter, nat, DDOS, searching FIB, Then the network traffic is handed to the output LPU.

1.5.1.2 Physical Architect

The physical architecture includes the following systems:

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

Except the network management system (NMS), all the other systems are in the integrated cabinet. The power distribution system works in 1+1 backup mode. The functional host system is the target of this evaluation and 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 is composed of the system backplane, SRUs/MPUs, LPUs, SPUs and SFUs. SRU/MPU are the boards hosting which provides control and management functionalities. LPU is the board containing the hash engine and responsible for network traffic QOS processing. Generally SRU/MPU are called MPU for simplicity in case of brief introduction.

The functional host system processes data. In addition, it monitors and manages the entire system, including the power distribution system, heat dissipation system, and NMS through NMS interfaces which are not within the scope of this evaluation.

The TOE provides several models. These models differ in their modularity and throughput but use the same version of software and have identical security functionality.

The TOE scope is listed in Table 1-6.

Table 1-6 TOE Scope

Type	Name	Version
Software	Product software	V300R001C01SPC300B113
	VRP	Version 5 Release 70
Hardware	Eudemon8000E-X3/Secospace USG9520	Refer to Table 1-7
	Eudemon8000E-X8/Secospace USG9560	Refer to Table 1-8
	Eudemon8000E-X16/Secospace USG9580	Refer to Table 1-9
Guidance	HUAWEI Eudemon8000E V300R001C01SPC300 Product Documentation	07

The binaries inside the product can be found in the Table 1-2.

Eudemon8000E-X3/Secospace USG9520 Chassis Overview

The Eudemon8000E-X3/Secospace USG9520 chassis have both AC and DC models. Figure 1-2 shows a DC chassis, and the Figure 1-3 shows an AC chassis.

Figure 1-2 Appearance of a DC chassis

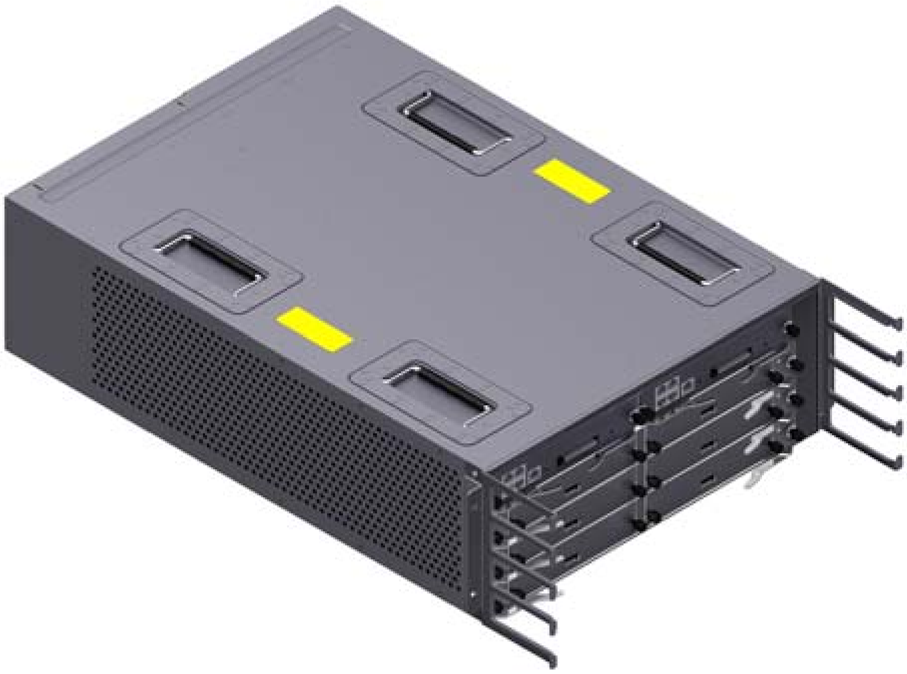


Figure 1-3 Appearance of an AC chassis

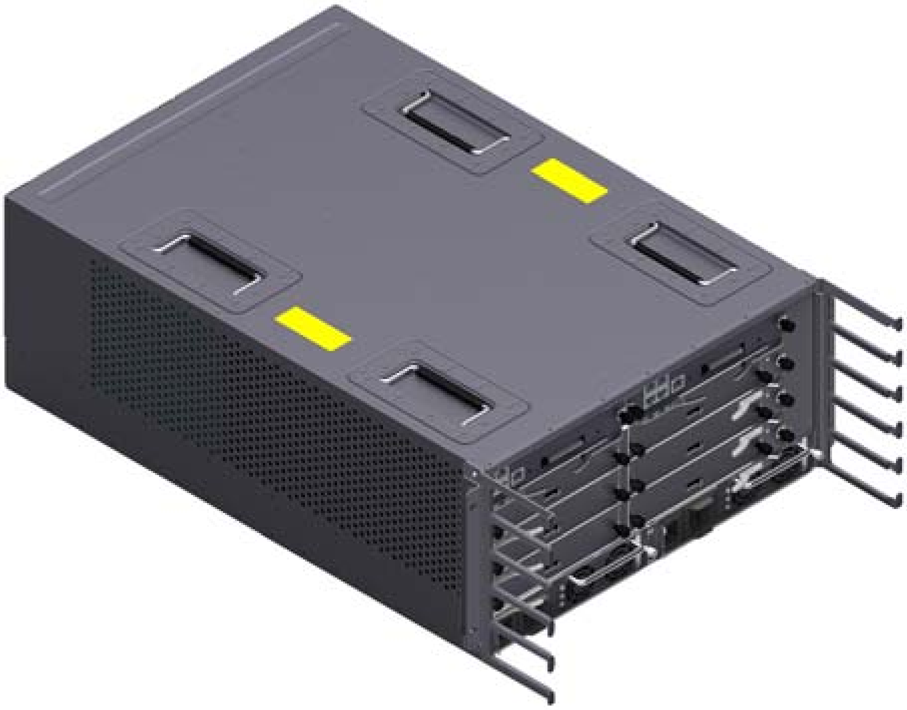


Figure 1-4 Diagram of the board slot area of the Eudemon8000E-X3/Secospace USG9520

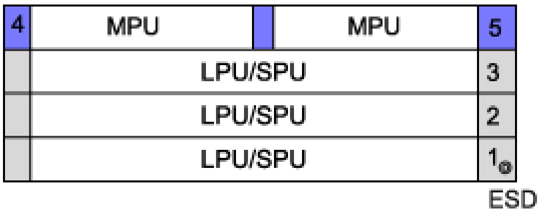


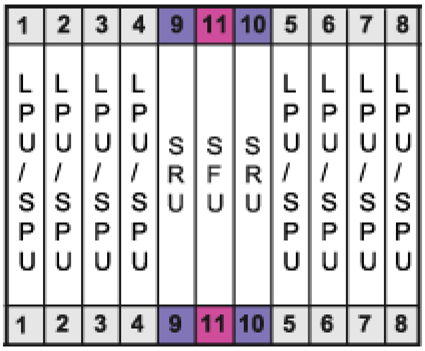
Table 1-7 Slot layout description of the Eudemon8000E-X3/Secospace USG9520

Slot	Quantity	Slot Width	Description
1 to 3	3	41 mm (1.6 inches)	Indicates the slots for Line Processing Units (LPUs) and Service Processing Units (SPUs). The LPUs and SPUs can co-exist to suit your requirements, but at least one LPU and one SPU are required.
4 to 5	2	41 mm (1.6 inches)	Indicates the slots dedicated for Main Processing Units (MPUs). The slot can house two MPUs to form 1:1 backup.

Eudemon8000E-X8/Secospace USG9560 Chassis Overview

Figure 1-5 Appearance of the chassis of the Eudemon8000E-X8/Secospace USG9560

Figure 1-6 Diagram of the board slot area of the Eudemon8000E-X8/Secospace USG9560



1	2	3	4	9	11	10	5	6	7	8
LPU/SPU	LPU/SPU	LPU/SPU	LPU/SPU	SRU	SFU	SRU	LPU/SPU	LPU/SPU	LPU/SPU	LPU/SPU
1	2	3	4	9	11	10	5	6	7	8

Table 1-8 Slot layout description of the Eudemon8000E-X8/Secospace USG9560

Slot	Quantity	Slot Width	Description

Table 1-8 Slot layout description of the Eudemon8000E-X8/Secospace USG9560

Slot	Quantity	Slot Width	Description
1 to 8	8	41 mm (1.6 inches)	Indicates the slots for LPUs and SPUs. The LPUs and SPUs can be inserted at the same time. Select the LPUs and SPUs as required, but at least one LPU and one SPU are required.
9 to 10	2	36 mm (1.4 inches)	Indicates two slots that are dedicated for Switch Router Units (SRUs). The slots can house two MPUs to form 1:1 backup.
11	1	36 mm (1.4 inches)	Indicates the slot for the Switch Fabric Unit (SFU). The SFU interworks with the SFU integrated on the SRU to form 2+1 backup for load-balancing.

Eudemon8000E-X16/Secospace USG9580 Chassis Overview

Figure 1-7 Appearance of the chassis of the Eudemon8000E-X16/Secospace USG9580

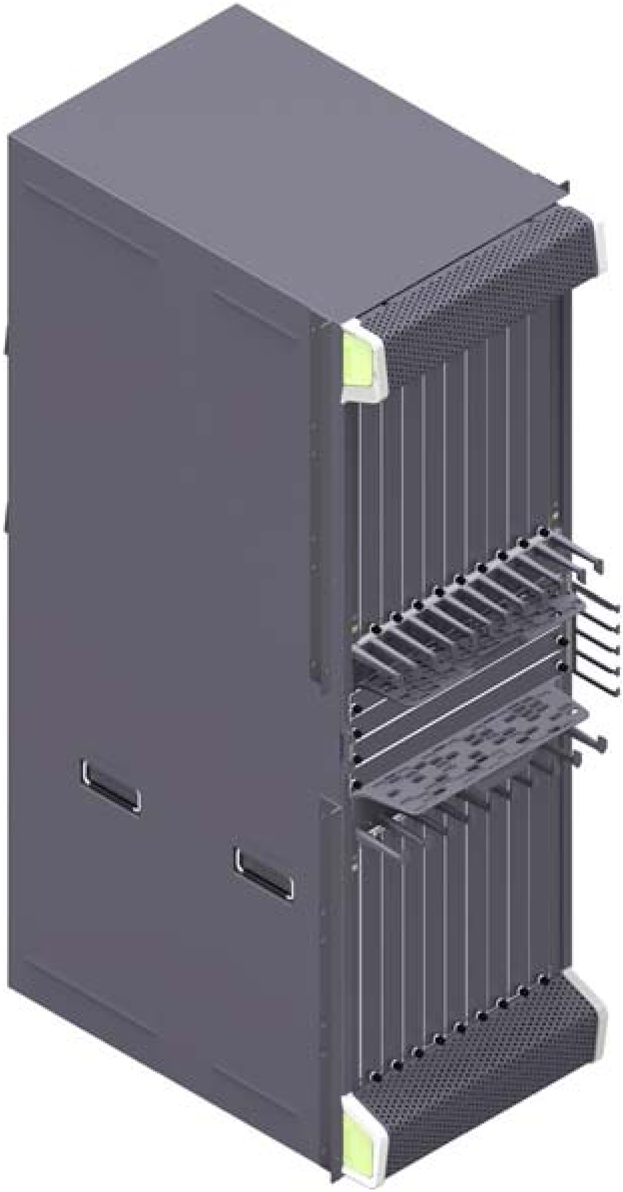


Figure 1-8 Diagram of the board slot area of the Eudemon8000E-X16/Secospace USG9580

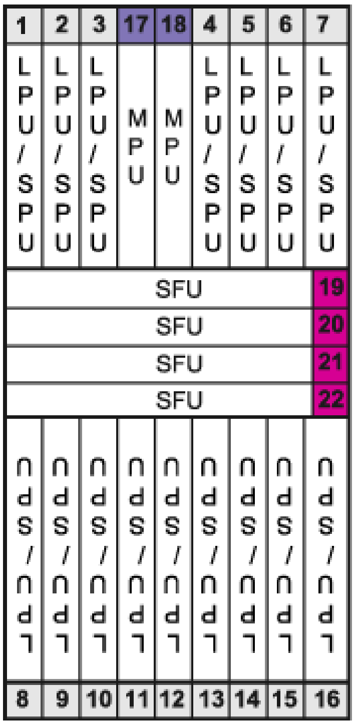


Table 1-9 Slot layout description of the Eudemon8000E-X16/Secospace USG9580

Slot	Quantity	Slot Width	Description
1 to 16	16	41 mm (1.6 inches)	Indicates the slots for LPUs and SPUs. The LPUs and SPUs can be inserted at the same time. Select the LPUs and SPUs as required, but at least one LPU and one SPU are required.
17 to 18	2	41 mm (1.6 inches)	Indicates the slots dedicated for MPUs. The slots can house two MPUs to form 1:1 backup.
19 to 22	4	41 mm (1.6 inches)	Indicates the slots for SFUs. The slots can house four SFUs to form 3+1 backup for load balancing.

1.5.1.3 Network Interface

The physical boundary of the TOE is the actual firewall 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.

Table 1-10 details all physical interfaces available in TOE along with respective usage:

Table 1-10 Interfaces Specifications

Boards	Supported Interfaces and Usage
MPU/SRU	The following list shows a collection of interfaces which might be used during this evaluation for all models. The description about indicators on panel can be found in the *Hardware Description of HUAWEI Eudemon8000E/USG9000 V300R001C01SPC300 Product Documentation 07*(http://support.huawei.com/ehedex/hdx.do?docid=DOC1000038501&lang=en：Description > Hardware Description> List of Boards). CF card interface, connector type TYPE II compatible with TYPE I, is used to hold a CF card to store data files as a massive storage device. The CF card is inserted and sealed within the TOE and is to be accessed only by authorized personnel. User configuration profiles, paf and licensing files, log data, system software and patches if exist are stored in the CF card. ETH interface, connector type RJ45, operation mode 10M/100M/1000M Base-TX auto-sensing, supporting half-duplex and full-duplex, compliant to IEEE 802.3-2002, used for connections initiated by users and/or administrators from a local maintenance terminal via SSH to perform management and maintenance operations. Management and maintenance on NMS workstation is not within the scope of this evaluation thus NMS related accounts should be disabled during the evaluation. Console interface, connector type RJ45, operation mode Duplex Universal Asynchronous Receiver/Transmitter (UART) with electrical attribute RS-232, baud rate 9600 bit/s which can be changed as required, used for users and/or administrators to connect to console for the on-site configuration of the system.
LPU	Interfaces supported by LPU are listed as below. More details about these interfaces can be found in the *Interface Attributes of HUAWEI Eudemon8000E/USG9000 V300R001C01SPC300 Product Documentation 07*(http://support.huawei.com/ehedex/hdx.do?docid=DOC1000038501&lang=en：Description > Hardware Description> List of Interface Attributes). ETH interface, connector type RJ45, operation mode 10M/100M/1000M Base-TX auto-sensing, supporting half-duplex and full-duplex, used for receiving and transmitting network traffic. FE interface, connector type LC/PC optical connector, compliant to SFP optical module 100M-FX, supporting full-duplex, used for receiving and transmitting network traffic. GE interface, connector type LC/PC optical connector, compliant to SFP optical module 1000Base-X-SFP, supporting full-duplex, used for receiving and transmitting network traffic. 10GE interface, connector type LC/PC optical connector, compliant to XFP optical module 10GBase LAN/WAN-XFP, supporting full-duplex, used for receiving and transmitting network traffic 40GE interface, connector type LC/PC optical connector, compliant to CFP optical module 40GBase LAN-CFP, supporting full-duplex, used for receiving and transmitting network traffic 100GE interface, connector type LC/PC optical connector, compliant to CFP optical module 100GBase CFP, supporting full-duplex, used for receiving and transmitting network traffic The following interfaces are supported by the TOE, but not to be evaluated in this evaluation. POS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-3c/STM-1c POS-SFP, supporting full-duplex, used for receiving and transmitting network

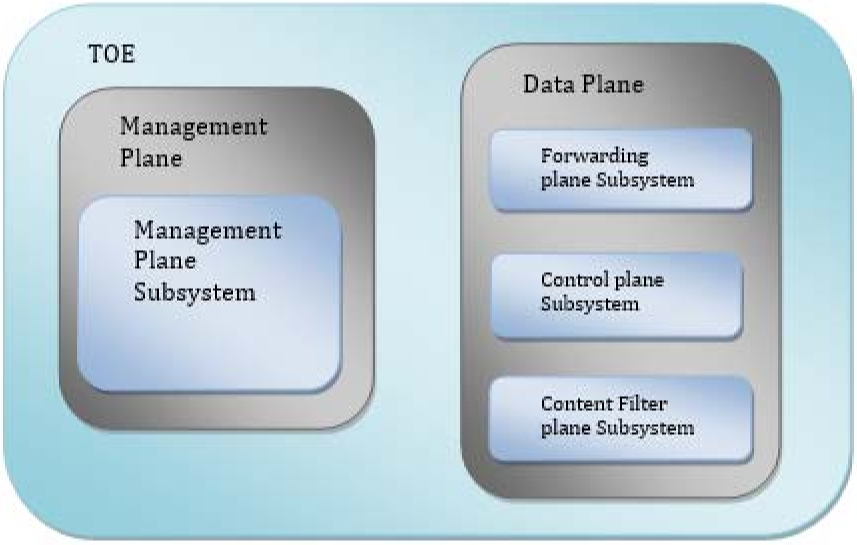
Boards	Supported Interfaces and Usage
	traffic. POS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-12c/STM-4c POS-SFP, supporting full-duplex, used for receiving and transmitting network traffic. POS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-48c/STM-16c POS-SFP, supporting full-duplex, used for receiving and transmitting network traffic. POS interface, connector type LC/PC optical connector, compliant to XFP optical module OC-192c/STM-64c POS-XFP, supporting full-duplex, used for receiving and transmitting network traffic. The network traffic being received and transmitted by these interfaces, can be further described as non-TSF data (information flow to be forwarded to other network interfaces and information flow destined to TOE but not security-related) and TSF data (destined to TOE for control and management purpose and for security-related functionalities). The definition for non-TSF data and TSF data will be further explained in Chapter 1.4.4.

1.5.2 Logical Boundary

1.5.2.1 Logical Architect

This section will describe the logical architect of the TOE in Figure 1-9.

Figure 1-9 TOE Software architecture


TOE
Management Plane
Management Plane Subsystem
Data Plane
Forwarding plane Subsystem
Control plane Subsystem
Content Filter plane Subsystem

The TOE software is divided into two different planes: Management Plane (MP) a Data Plane (DP). MP is composed by only one subsystem called Management plane Subsystem. DP is composed by three subsystems called Forwarding plane Subsystem, Control plane Subsystem**,** and Content Filter Subsystem.

Management plane subsystem provides configuration management, protocol, status, routing management and device management. (**Security Function Management, Cryptographic support, Access control, Authentication, Communication Security**)

Forwarding plane subsystem provide firewall packet forwarding, security check and traffic control. (**Flow control policy, Communication Security**)

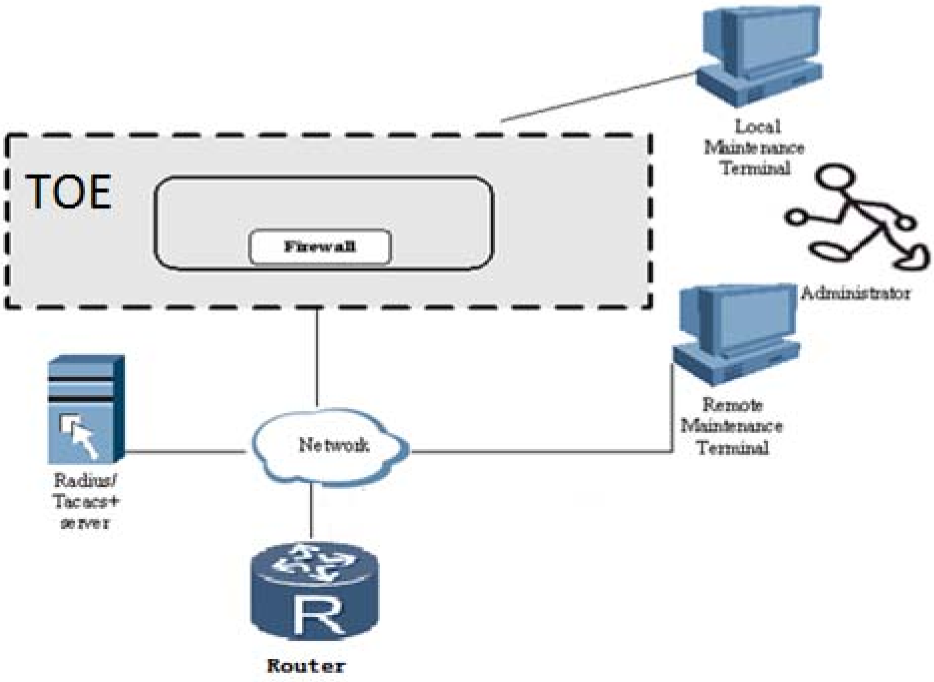
Control plane subsystem provides user authentication(local or remote using a RADIUS or TACACS server), relation analyze and remote query for specific operation. (**Authentication, Communication security**)

Content Filter plane subsystem provides functionality which is not SFR-related such as anti-virus, anti-spam, DPI (Deep Protocol Identification), and other non-security features. This subsystem is irrelevant with the security features, and therefore will no longer be mentioned along this security target.

1.5.3 TOE Environment

Figure 1-10 shows the TOE's logical scope with supporting network devices of the environment.

Figure 1-10 TOE logical scope



The environment for TOE comprises the following components:

- An optional Radius or TACACS+ server providing authentication and authorization decisions to the TOE (it must be compatible with L2TP[VPN], IPSEC[VPN] and x.509 certificates).

- Peer routers providing routing information to the TOE via dynamic protocols.
- 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 the administrator to connect to the TOE to manage it. These connections are performed via a secure channel enforcing HTTP over SSL/TLS. It is required to install the https client on these PCs.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.

2 CC Conformance Claim

This ST is CC Part 2 conformant and CC Part 3 conformant. The CC version of [CC] is 3.1R4.

No conformance to a Protection Profile is claimed.

No conformance rationale to a Protection Profile is claimed.

The TOE claims EAL3+ augmented with ALC_CMC.4 + ALC_CMS.4.

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, 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.

Table 1-11 Information Assets

	Confidentiality	Integrity	Availability
Log data	X	X	X
Configuration data	X	X	X
Traffic through the TOE			X
User interaction traffic	X	X	X

Table 1-12 lists the threats addressed by the TOE and the IT Environment.

Table 1-12 Threats

Threat Name	Threat Definition
T.UnwantedTraffic	Any network user that sends unwanted/unexpected traffic to/through the TOE will: cause the TOE and/or resources on the network to become too slow or unavailable, or reach resources on the network that it is not allowed to reach.

T.UnauthenticatedAccess	A user who is not an administrator gains access to the management interface of the TOE
T.UnauthorizedAccess	An administrator authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
T.Eavesdrop	An eavesdropper is able to intercept, and potentially modify or re-use information assets that are exchanged between: TOE and LMT/RMT (management traffic) TOE and other routers/switches (routing information)

3.2 Assumptions

Table 1-13 TOE Assumption

Assumption Name	Assumption Definition
A.PhysicalProtection	The TOE is physically protected so that only the authorized user of the TOE has physical access.
A.NetworkElements	The environment is supposed to provide supporting mechanism to the TOE: • A Radius server or TACACS+ server for external authentication/authorization decisions; • Peer router(s) for the exchange of dynamic routing information; • Remote entities (PCs) used for administration of the TOE.
A.NetworkSegregation	It is assumed that the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE.
A.NoEvil	The administration users who manage the TOE and TOE environmental components are appropriately trained, non-hostile, and follow all guidance.

4 Security Objectives

4.1 Objectives for the TOE

Table 1-14 Security Objectives for the TOE

TOE Security Obj.	Definition
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 shall protect the network communication between: the TOE and LMT/RMT (management information) the TOE and other switches/routers (routing information)
O.Authorization	The TOE shall allow different authorization levels to be assigned to administrators in order to restrict the functionality that is available to individual administrators.
O.Authentication	The TOE shall authenticate users before allowing them access to its management interface

4.2 Objectives for the Operational Environment

Table 1-15 Security Objectives for the Operational Environment

Environment Security Objective	Definition
OE.NetworkElements	The operational environment shall provide network devices that the TOE needs to cooperate with: • A Radius server or TACACS+ server for

Environment Security Objective	Definition
	external authentication/authorization decisions; • Peer router(s) for the exchange of dynamic routing information; • Remote entities (PCs) used for administration of the TOE.
OE.Physical	The operational environment shall protect the TOE against unauthorized physical access.
OE.NetworkSegregation	The operational environment shall ensure that hat the ETH interface in the TOE will be accessed only through an independent local network This network is separate from the networks that use the other interfaces of the TOE.
OE.Manage	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.

4.3 Security Objectives Rationale

Table 1-16 Rationale for threats

Threat	Rationale for security objectives to 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). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits
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
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

Threat	Rationale for security objectives to threats
	Server. (O.Communication).

Table 1-17 Rationale for assumptions

Assumption	Rationale for security objectives
A.NetworkElements	Directly covered by OE.NetworkElements.
A.PhysicalProtection	Directly covered by OE.Physical.
A.NetworkSegregation	Directly covered by OE.NetworkSegregation.
A.NoEvil	Directly coverd by OE.Manage

Table 1-18 Mapping of Objectives to Threats and Assumptions

	T.UnwantedTraffic	T.UnauthenticatedAccess	T.UnauthorizedAccess	T.Eavesdrop	A.NetworkElements	A.PhysicalProtection	A.NetworkSegregation	A.NoEvil
O.DeviceAvail	X							
O.UserAvail	X							
O.DataFilter	X							
O.Communication				X				
O.Authorization			X					
O.Authentication		X						
OE.NetworkElements					X			
OE.Physical						X		
OE.NetworkSegregation							X	

OE.Manage								X

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/N indicates an element of the iteration, where N is the iteration number/character.

6.2 TOE Security Functional Requirements

6.2.1 Cryptographic Support (FCS)

6.2.1.1 FCS_COP.1/AES Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[symmetric encryption/decryption]** in accordance with a specified cryptographic algorithm **[AES CBC Mode]** and cryptographic key sizes **[128bits, 192bits, 256bits]** that meet the following: **[none]**

6.2.1.2 FCS_COP.1/3DES Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[symmetric encryption/decryption]** in accordance with a specified cryptographic algorithm **[3DES Outer CBC Mode]** and cryptographic key sizes **[168bits]** that meet the following: **[none]**

6.2.1.3 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[asymmetric encryption/decryption]** in accordance with a specified cryptographic algorithm **[RSASSA-PKCS-v1_5 with SHA1]** and cryptographic key sizes **[512bits-2048bits]** that meet the following: **[none]**

6.2.1.4 FCS_COP.1/HMAC-SHA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[message authentication code calculation]** in accordance with a specified cryptographic algorithm [**HMAC-SHA**] and cryptographic key sizes **[20 bytes]** that meet the following: **[none**].

6.2.1.5 FCS_CKM.1/AES Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Diffie-Hellman Key Exchange]** and specified cryptographic key sizes [**128/192/256 bits]** that meet the following: **[none].**

6.2.1.6 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 **[Diffie-Hellman Key Exchange]** and specified cryptographic key sizes [**168 bits**] that meet the following: **[none]**

6.2.1.7 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 **[512bits-2048bits]** that meet the following: **[none]**

6.2.1.8 FCS_CKM.1/HMAC-SHA Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Diffie-Hellman Key Exchange]** and specified cryptographic key sizes **[20 bytes]** that meet the following: **[none]**

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1 Subset access control

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

[Subject: all level users refer to Table 1-4;

Objects: commands /features provided by TOE;

Operation: execute]

6.2.2.2 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:**[**

Security attributes are for subject users:

- **user level**

Objects security attributes:

- **command level]**

Note: The particular user with name “admin” is built in.

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) **The TSF checks the level of the user and the level of the command, and allow this user access to the command if the level of the command is less than or equal this level of user.**

b) **The TSF checks the level of the user and the level of the command, and deny this user access to the command if the level of the command is greater than this level of user.]**

Note: Above mentioned information is identified in Table 1-4.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none**].

6.2.2.3 FDP_IFC.1 Subset information flow control

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

[**subjects: external IT entities that send and receive information through the TOE to one another;**

information: traffic sent through the TOE from one subject to another;

and

operations: permit or deny access information].

6.2.2.4 FDP_IFF.1 Simple security attributes

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

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

subject security attributes:

• none;

information: traffic sent through the TOE from one subject to another;

information security attributes:

- **IP.protocol**
- **IP.flags**
- **IP.fragment_offset**
- **IP.source_address**
- **IP.destination_address**
- **(TCP/UDP).source_port**
- **(TCP/UDP).destination_port**
- **presumed address of source subject;**
- **presumed address of destination subject;**
- **presumed port of source subject;**

• presumed port of destination subject;

• transport layer protocol;

• next protocol identifier;

• fragment identifier;

].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[**

- **the information match the flow control policy;**
- **the flow control policy action is permitted;]**

FDP_IFF.1.3 The TSF shall enforce the **[none]**.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **[**

a) **IP.protocol==IPPROTO_TCP &&TCP.destination_port = (179|646)**
b) **IP.protocol==IPPROTO_OSPF &&IP.flags indicates more fragments (see iprfc) &&IP.fragment_offset> 0**

]

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:[

a) **all the information security attributes match the information flow control policy and the action for matched information flow is denied;**

b) **if any of the information attributes identified in FDP_IFF.1.1 do not match the attributes of the flow control policy;**]

6.2.3 Identification and Authentication (FIA)

6.2.3.1 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;**].

6.2.3.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.3 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to[***modify the behaviour of***] the functions **[all the defined in FMT_SMF.1]** to **[management level users refer to Table 1-4**] .

6.2.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**access control policy**] to restrict the ability to [***modify***] the security attributes [**identified in FDP_ACF.1**] to [**management level users refer to Table 1-4**].

6.2.4.3 FMT_MSA.3 Static attribute initialization

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

Note: There is not any privilege for the user just created by default.

FMT_MSA.3.2 The TSF shall allow the [**management level users refer to Table 1-4]** to specify alternative initial values to override the default values when an object or information is created.

Note: The commands are fixed by design. The commands cannot be created by the admin users. The only attribute that can be modified later, only by a manager user, is the command level.

6.2.4.4 FMT_SMF.1 Specification of Management Functions

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

a) **flow control policy**

b) **user management**

c) **SSH**

d) **CPCAR**

e) **routing management**

Note1: The authentication and authorization are enabled by design, and can’t be disabled.

Note2: The flow control policy is enabled by design and can’t be disabled.

Note3: The user management is enabled by design and can’t be disabled.

Note4: The CPCAR is enabled by design and can’t be disabled.

Note5: The routing management is enabled by design and can’t be disabled.

Note6: The clock management is enabled by design and can’t be disabled.

6.2.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**visit level users, monitoring level users, configuration level users and management level users refer to Table 1-4**].

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

6.2.5 TOE access (FTA)

6.2.5.1 FTA_SSL.3 TSF-initiated termination

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

6.3 Security Functional Requirements Rationale

6.3.1 Sufficiency and coverage

Table 1-19 Objectives to SFR mapping rationale

Objective	SFRs	Rationale
O.DeviceAvail	FDP_IFC.1 FDP_IFF.1	These SFRs apply flow control policy to process packets sent to the CPU, ensuring device security and uninterrupted services when attacks occur.
O.UserAvail	FDP_IFC.1 FDP_IFF.1	These SFRs apply flow control policy to process packets sent to the CPU, ensuring device security and uninterrupted services when attacks occur.
O.Communication	FCS_COP.1/* FCS_CKM.1/*	These SFRS provide the cryptographic services for the secure communication above.
O.DataFilter	FDP_IFC.1 FDP_IFF.1	These SFRs apply flow control policy to limit both packets going to the Control/Management Plane and through the TOE and thereby ensure that protected traffic goes through.
O.Authentication	FIA_UID.2 FIA_UAU.2	These SFRs ensure that a user must identify and authenticate himself, either by local password or through RADIUS/TACACS servers.
	FTA_SSL.3	The SFRs support authentication by: Logging out users after an inactivity period Ensuring password quality
O.Authorization	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.

Objective	SFRs	Rationale
	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.

Table 1-20 Mapping of SFRs to Objectives

	O.DeviceAvail	O.UserAvail	O.Communication	O.DataFilter	O.Authentication	O.Authorization
FDP_IFC.1	X	X		X		
FDP_IFF.1	X	X		X		
FDP_ACC.1						X
FDP_ACF.1						X
FIA_ATD.1						X
FIA_UAU.2					X	
FIA_UID.2					X	
FMT_MOF.1						X
FMT_MSA.1						X
FMT_MSA.3						X
FMT_SMF.1						X
FMT_SMR.1						X
FTA_SSL.3					X	
FCS_COP.1/*			X			
FCS_CKM.1/*			X			

6.3.2 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. There are some dependencies that are not resolved directly with any SFRs, in these cases an application note is required. This application note is included below the following table:

Table 1-21 Dependencies between TOE Security Functional Requirements

Security Functional Requirement	Dependencies	Resolution
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No Dependencies	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	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] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 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.2
FTA_SSL.3	No Dependencies	None
FCS_COP.1/AES Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/AES Cryptographic key generation FCS_CKM.4 see Application Note below
FCS_COP.1/3DES Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/3DES Cryptographic key generation FCS_CKM.4 see Application Note below
FCS_COP.1/RSA Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or	FCS_CKM.1/RSA Cryptographic key generation

Security Functional Requirement	Dependencies	Resolution
	FCS_CKM.1] FCS_CKM.4	FCS_CKM.4 see Application Note below
FCS_COP.1/HMAC-SHA Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/HMAC_SHA Cryptographic key generation FCS_CKM.4 see Application Note below
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 see Application Note below
FCS_CKM.1/3DES Cryptographic key generationFCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4F CS_COP.1	FCS_COP.1/3DES Cryptographic operation FCS_CKM.4 see Application Note below
FCS_CKM.1/RSA Cryptographic key generationFCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4 FCS_CKM.4	FCS_COP.1/RSA Cryptographic operation FCS_CKM.4 see Application Note below
FCS_CKM.1/HMAC_SHA Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/HMAC-SHA Cryptographic operation FCS_CKM.4 see Application Note below

Application Note: A key deletion active procedure is not provided by the TOE. However, the TOE performs a memory freeing procedure in association with memory isolation between the different processes. This memory isolation is reached using dynamic TLB settings between the processes.A TLB entry is for enabling and limiting the memory access for specific process. With different TLB settings, which means, different memory scope for the processes, there is no memory overlaps between them. In this way, a different memory part is assigned to each process, and they cannot share their memory with other process. Therefore, the memory where the key is stored is not accessible by other process.

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are EAL3+ augmented with ALC_CMC.4 + ALC_CMS.4 components as specified in [CC] Part 3. No operations are applied to the assurance components.

Assurance class	Assurance components
Development	ADV_ARC.1 Security architecture description

Assurance class	Assurance components
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_TSS.1 TOE summary specification
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_VAN.2 Vulnerability

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 3+ ALC_CMC.4 + ALC_CMS.4 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

7.1.1 Authentication and Identification

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 server. This function is achieved by performing pass/fail action based on result from remote RADIUS authentication server.

3 Support authenticate user login using SSH, by password authentication, RSA authentication, or combination of both. This function is achieved by performing authentication for SSH user based on method mentioned in 1.

4 Support remotely authenticate user login using HTTPS through the Web-Based GUI.

5 Support logout when no operation is performed on the user session within a given interval.

6 Support manual session termination by username. This function is achieved by interpreting commands for username, locating and cleaning session information related to this username, forcing this username to re-authenticate.

7 Support authentication via corresponding administrator level.

(FCS_COP.1/RSA, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTA_SSL.3)

7.1.2 Access Control

The TOE enforces an access control by supporting following functionalities:

1 Support assigning command level (0-3).

2 Support assigning user level (0-15).

3 Users can perform commands only when the user level is greater or equal than the command level. This limitation of access also prevents users from accessing or deleting log files if they have insufficient rights.

4 Support enforcing the access control policy based on security attributes of users.

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

7.1.3 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. STelnet are provided implementing secure Telnet and FTP, to substitute Telnet and FTP which are deemed to have known security issues.

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 and AES encryption algorithm. This function is achieved by providing implementation of 3DES, AES algorithm.

4 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.

5 Support Secure-TELNET. This function is achieved by providing implementation of Secure-TELNET.

6 Support Secure-FTP. This function is achieved by providing implementation of Secure-FTP.

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

7.1.4 Flow Control Policy

7.1.4.1 Logical Relationship of the Flow Control Policy

After receiving a packet, the device extracts the IP header information, including source and destination IP addresses, protocol, and priority, and compares the information with the matching conditions of the interzone flow control policy. If all matching conditions are met, the device conducts security check on the packet based on the policy control action (permit or deny), and processes the packet accordingly.

When no condition is defined in the policy, and only the action is defined, the policy matches any packets.

7.1.4.2 Composition of the Flow Control Policy

Each flow control policy comprises the matching conditions and control action.

Matching condition

The matching conditions of a flow control policy are as follows:

- Source/destination IP address
- Service type of an IP packet: limits the port or protocol type.
- Time range: Controlled traffic is permitted within a given time range.
- Precedence field in an IP packet
- ToS field in an IP packet

A flow control policy specifies multiple matching conditions. A packet meeting all conditions can match the policy.

You can set multiple values for one matching condition. For example, you can set multiple source IP addresses. In this case, traffic meets the matching condition only if one source IP address is matched.

Control action

Two actions are available for flow control policies:

- permit: allows the packet to pass the check of flow control policies.
- deny: discards the packet

7.1.4.3 The Functionality Associated to Flow Control Policy

The TOE supports flow control policy to filter traffic destined to TOE to prevent internal traffic overload and service interruption. The TOE also uses the IP-Car policy perform flow control to prevent the CPU and related services from being attacked.

- Support screening, filtering traffic destined to CPU. This function is achieved by downloading policy configurations into hardware.
- Support rate limiting traffic based on screened traffic. This function is achieved by downloading configuration of rate into hardware.
- Support configuration based on IP protocol number, source and/ordestination IP address, source and/or destination port number if TCP/UDP.

(FMT_SMF.1, FDP_IFC.1, FDP_IFF.1)

7.1.5 Security Management

The functionality in the TOE requires management to ensure proper configuration control.

The TOE restricts to a visit level users, monitoring level users, configuration level users and management level users refer to Table 1-4 with appropriate privileges the ability to modify the number of failed authentication attempts via CLI Login that occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.

The TOE is delivered with restrictive default values such that no traffic can pass across the TOE until specific configuration changes are made.

To enable forwarding between directly connected networks the IP addresses of the TOE interfaces must be configured.

The TOE will not route to an indirectly connected subnet (through another routing device) unless a route is configured in the TOE.

The CLI provides a text-based interface from which the TOE configuration can be managed and maintained. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

From the CLI interface new accounts can be created, and existing accounts can be modified or deleted. This interface also provides the management level user and configuration level user with the ability to configure an external authentication server, such as a RADIUS or TACACS+ server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE.

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:

1 User management, including user name, passwords, etc.

7 Routing management.

8 Access control policy management, including the association of users and corresponding privileged functionalities.

9 Enabling/disabling of SSH for the communication between LMT clients and the TOE.

10 Defining IP addresses and address ranges for clients that are allowed to connect to the TOE.

11 Support configuration flow control policy based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;

12 Support to set the user default privileges, and modify user privileges;

13 Support configuration for CPCAR;

All of these management options are typically available via the LMT GUI.

(FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FMT_MOF.1)

7.1.6 Cryptographic Functions

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

1 Support AES/3DES/RSA algorithms. This is achieved by providing implementations of AES/3DES/RSA algorithms.

2 Support HMAC-SHA algorithm. This is achieved by providing implementations of HMAC-SHA algorithms

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

8 Abbreviations, Terminology and References

8.1 Abbreviations

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
CC	Common Criteria
CFM	Connectivity Fault Management
CLI	Command Line Interface
CPCAR	Control Plane Committed Access Rate
DSA	Digital Signature Algorithm
FTP	File Transfer Protocol
GUI	Graphical User Interface
IC	Information Center
LMT	Local Maintenance Terminal
LPU	Line Process Unit
MPU	Main Processing Unit
NTP	Network Time Protocol
PP	Protection Profile
RM	Routing Management
RMT	Remote Maintenance Terminal

RSA	Rivest Shamir Adleman
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SNMP	Simple Network Management Protocol
SPU	Service Process Unit
SRU	Switch Router Unit
SSH	Secure Shell
ST	Security Target
STP	Spanning Tree Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
VP	Virtual Path
VRP	Versatile Routing Platform
VTY	Virtual Type Terminal

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.

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.

[CEM] Common Methodology for Information Technology Security Evaluation. Version 3.1 Revision 4.