Eudemon1000E-N(USG6600) Series Firewall — Security Target

Version: 1.13

Last Update: 2015-10-28

Author: Huawei Technologies Co., Ltd.

Revision record

Date	Revision Version	Change Description	Author
2013-09-14	0.1	Initial Draft	sungang 57594
2013-10-23	0.2	Update product information	sungang 57594
2013-12-10	0.3	Update product information	sungang 57594
2014-03-05	0.4	Update product information	sungang 57594
2014-04-03	0.5	Update product information and system architecture information	sungang 57594
2014-05-04	0.6	Update information	sungang 57594
2014-06-03	0.7	Update information	sungang 57594
2014-06-10	0.8	Split to 2 STs	sungang 57594
2014-07-28	0.9	Update information	Sungang 00288227
2014-08-11	1.0	Update information	Sungang 00288227
2014-09-04	1.1	Update version to C20	Sungang 00288227
2014-09-09	1.2	Update information for EE comments	Sungang 00288227
2014-09-12	1.3	Update information for EE comments	Sungang 00288227
2014-11-17	1.4	Remove BGP/OSPF related SFR information.	Sungang 00288227
2015-01-05	1.5	Update information for EE comments	Sungang 00288227
2015-01-27	1.6	Add the P/N number information to the TOE	Sungang 00288227
2015-01-29	1.7	Add 2 comments to describe the version identifier.	Sungang 00288227
2015-3-3	1.8	Update information for ATE review 2015/2/18	Sungang 00288227
2015-6-27	1.9	Update information for ATE review 2015/5/13	Sungang 00288227
2015-7-8	1.10	Update information.	Sungang 00288227
2015-8-9	1.11	Update information	Sungang 00288227
2015-10-1	1.12	Update information	Sungang 00288227
2015-10-28	1.13	Update information	Sungang 00288227

Table of Contents

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is HuaweiEudemon1000E-N(USG6600) Series Firewall, and will hereafter be referred to as the TOE throughout this document. The TOE is a hardware system, which can provide Firewall, VPN, antivirus protection, anti-spam protection and content filtering etc. to provide network protection.

1.1 Security Target Identification

Name: Eudemon1000E-N(USG6600) Series Firewall - Security Target

Version:1.13

Publication Date: 2015-10-28

Author: Huawei Technologies Co., Ltd.

1.2 TOE Identification

A) TOE name:

Eudemon1000E-N(USG6600) Series Firewall

B) Evaluated platforms:

Series Id	**Model Name**	**ESN**
Eudemon 1000E/USG	Eudemon1000E-N7E	210235G7FYZ0C8000001

6600	USG6620	2102359519Z0C9000004
	USG6650	210235G7G410E7000104
	USG6680	210235G7G70123401230

C) SW version and Binary identifier

All platforms list above are running the same software.

V100R001C20SPC100B021 VxWorks 5.5.2 WindriverLinux 4.3 (Kernel 2.6.34.10)	File name: sup.bin MD5: 1365AF8E1D3B0261CF8461CD281EF493

1.3 Product Overview

Eudemon1000E-N(USG6600) Series Firewall, the TOE is a hardware platform and software image integrated as a whole system. It is designed to providefirewall, IPv6, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, anti-spam protection and content filteringetc. 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 ofrules) defined by the Security Administrator. They detect and eliminate the most damaging,content-based threats from email and Web traffic such as viruses, worms, intrusions,inappropriate Web content and more in real-time; without degrading network performance.In addition to providing stateful application-level protection, the TOE delivers a full range of network-level services including; firewall, IPv6, VPN, VLAN, antivirus protection, anti-spamprotection and content filtering etc.; using dedicated, easily managed platforms.

All these security features are out of the CC evaluation, and therefore no assurance is claimed over them.

1.4 Target of Evaluation (TOE) Overview

Eudemon1000E-N(USG6600) Series Firewall, the TOE provides high-end networking capacities for telecom and enterprise core networks. It consists of both hardware of software.

The TOE, provides the following major security features: authentication, access control, communication security, flow control policy, security functionality management, cryptographic functions. These security features are described below.

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

The major security features provided by the TOE are: authentication, access control, communication security, flow control policy, security functionality and cryptographic functions. During the description of these security features, there are some references to features that are not included in the evaluated configuration, e.g. Telnet or FTP. For those features, that are explicitly

mentioned, there is no security guarantee associated with them.

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 ConsoleCLI or remotely using the Network Web-Based GUI or Network CLI. The TOE provides a local authentication scheme for this, or can optionally enforceauthentication decisions obtained from a Radius or TACACS+ server in the ITenvironment.Authentication is always enforced for network remote sessions via SSH, SFTP (Secure FTP),andHTTPS (Web-Based GUI) sessions. Authentication for access via the console is always enabled and password protected.

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

1.4.2.2 Access Control

The TOE has the ability to control the administrator permissions for every administrator account. This control is performed using three different control policies: administrator roles, administrator levels and users built-in.

In order to determine the permissions associated to an administrator account, the TOE establishes the following priority between the control policies:

1. Users built-in.
2. Administrator roles.
3. Administrator levels.

These control policies are described in the following sections.

1.4.2.2.1 Administrator roles and levels

The TOE controls access by administrator roles and levels. Every administrator role has a list of read-write permissions, read-only permissions or none permissions. Four built-in hierarchical access control roles are offered that can be assigned to individual user accounts.

The TOE can also control the access by administrator levels. It controls the administrator permissions based on command levels.

Administrator Level	**Default administrator Role**	**Command Level**	**Permission Control Modules**		
			Read-Write	**Read-Only**	**None**

none	none	none	none	none	none
0	none	Allows access to visit-level commands.	none	none	none
1	device-admin(monitor)	Allows access to visit- and monitor-level commands.	none	• Dashboard • Monitor: - Report table - Traffic Map - Threat Map - Session Table - System Statistics - Quintuple Packet Discarding Statistics - Log • Log module, including the following submodules: - Traffic Log - Threat Log - URL Log - Content Log - User Activity Log - Policy	• Monitor: - Quintuple Packet Capture - Diagnosis Center - Audit Log • Log module, including the following submodules: - Operation Log - System Log - Audit Log • Policy module, including the following submodules: - Audit

				Matching Log - Mail Filtering Log	Policy • Object module, including the following submodules: - Audit Configuration • System module, including the following submodules: - Setup - Admin
2	device-admin	Allows access to visit-, monitor-, and configuration-level commands.	• Policy module, including the following submodules: - Security Policy - NAT Policy - Bandwidth Management - Quota	• Dashboard • Monitor: - Report table - Traffic Map - Threat Map - Session Table - System Statistics - Quintuple Packet Discarding Statistics	• Monitor - Quintuple Packet Capture - Diagnosis Center - Audit Log • Policy module, including the following submodule

			Control Policy - SSL Decryption Policy - Authentication Policy - Security Protection - ASPF Configuration • Object module, including the following submodules: - Certificates - Address - Region - Service - Application - User - Authenticati	- Log • Log module, including the following submodules: - Traffic Log - Threat Log - URL Log - Content Log - User Activity Log - Policy Matching Log - Mail Filtering Log	s: - Audit Policy - Object module, including the following submodules: - Audit Configuration • The log module, including the following submodules: - Operation Log - System Log - Audit Log • System module, including the following submodules: - Setup

			on Server - Schedule - URL Categories - Keyword Groups - Email Address Group - Signature - Link Health Check - Security Profiles Network module, including the following submodules: - Interface - Interface Pair - Zone - DNS - DHCP Server - Router		- Admin - Virtual system - Agile Network Configuration - Set Mail Service - License Management - Upgrade Center - System Upgrade - Configuration File Management - Audit Log Password Management

			- IPSec - L2TP - GRE - DSVPN - SSL VPN - TSM Interworking • System module, including the following submodules: - High Availability - Log Configuration - Configuration file modification • Other: - delete log		
3	system-admin	Allows access to visit-, monitor-, configuration-, and management-level commands.	• Dashboard • Monitor: - Report table - Traffic Map	none	• Monitor: - Audit Log • Log module, including

4~15	system-admin	Has the same permissions as the level-3 administrator. If the command line level is elevated, the administrator level (4 to 15) works with the elevated command line level.	- Threat Map - Session Table - System Statistics - Quintuple Packet Capture - Quintuple Packet Discarding Statistics - Diagnosis Center Log • Log module, including the following submodules: - Traffic Log		the following submodules: - Audit Log • Policy module, including the following submodules: - Audit Policy • Object module, including the following submodules: - Audit Configuration • System module, including the following submodules: - Audit Log Password Manag

			- Threat Log - URL Log - Content Log - Operation Log - System Log - User Activity Log - Policy Matching Log - Mail filtering Log • Policy module, including the following submodules: - Security Policy - NAT Policy - Bandwidth Management - Quota Contro		ement

			l Policy - SSL Decryption Policy - Authentication Policy - Security Protection - ASPF Configuration • Object module, including the following submodules: - Certificates - Address - Region - Service - Application - User - Authentication		

			Server - Schedule - URL Categories - Keyword Groups - Email Address Group - Signature - Link Health Check - Security Profiles • Network module, including the following submodules: - Interface - Interface Pair - Zone - DNS - DHCP Server		

			- Router - IPSec - L2TP - GRE - DSVPN - SSL VPN - TSM Interworking • System module, including the following submodules: - Setup - Admin - Virtual System - High Availability - Agile Network Configuration - Set Mail Service - Log Configuratio		

			n - License Management - Update Center - System Upgrade - Configuration file Management • Others: - delete log		
15	audit-admin	Configures a dedicated administrator role for auditing policies and viewing audit logs.	• Monitor: o Audit Log • Log module, including the following submodules: o Audit log • Policy module, including the following submodules: o Audit policy • Object module,	• Dashboard • Monitor: o Report table, o Traffic map o Threat map o Log • Log module, including the following submodules: o Traffic log o Threat log o URL log o Content log o Operation log o System log o User activity log o Policy matching log	• Monitor: o Quintuple Packet Capture o Quintuple Packet Discarding Statistics o Session Table o System Statistics o Diagnosis Center • Policy module, including the following submodules: o Security

			including the following submodules: o Audit configuration • System module, including the following submodules: o Audit Log Password Management • Others: o delete log	o Mail filtering log • System module o Discover CF cards contents	Policy o NAT Policy o Bandwidth Management o Quota Control Policy o SSL Decryption Policy o Authentication Policy o Security Protection o ASPF Configuration • Object module, including the following submodules: o Certificates o Address o Region o Service o Application o User o Authentication Server o Schedule o URL Categories o Keyword Groups o Email Address Group o Signature o Link Health Check o Security Profiles

					• Network module, including the following submodules: o Interface o Interface Pair o Zone o DNS o DHCP Server o Router o IPSec o L2TP o GRE o DSVPN o SSL VPN o TSM Interworking • System module, including the following submodules: o Setup o Admin o Virtual System o High Availability o Agile Network Configuration o Set Mail Service o Log Configuration o License Management o Update

					Center o System Upgrade o Configuration file Management

1.4.2.2.2 Built-in users

The TOE has also two special user that are built-in. The username of these users are *admin* and *audit-admin*, and they are associated to the *system-admin* role and the *audit-admin* role respectively. In addition, these users have the maximum administrator level (15). Permissions for these users must not be modified and they must not be removed from the TOE.

1.4.2.3 Communication Security

The TOE provides communication security by implementing SSH protocol. Twoversions of SSH: SSH1 (SSH1.5) and SSH2 (SSH2.0) are implemented. But SSH2 isrecommended for most cases by providing more secure and effectiveness in terms offunctionality and performance.

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

- authentication by password and by RSA;
- DES/3DES/AES encryption algorithms;
- Secure cryptographic key exchange.

Moreover, the communication security between the TOE and the web browser from the RMT (Remote Maintenance Terminal) is ensured by SSL/TLS protocol, thus these communications are performed over HTTPS instead of HTTP.

On the other hand, besides the default TCP port 22, manually specifying a listening port is also implementedsince it can effectively reduce attack.STelnet and SFTP are provided implementing secure Telnet and FTP, to substituteTelnet and FTP which are deemed to have known security issues.Moreover, both of them, Telnet and FTP, are disabled in the evaluated configuration, and therefore there is no security guarantee associated with these features.

Note: The connection between the TOE and the RADIUS/TACACS serverhas to be over an IPSec tunnel.

1.4.2.4 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. The administrator can create, delete, and modify rules for ACL configuration to prioritize, rate-limit the information flow destined to TOE 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.

Information flow that is processed with ACL and to be forwarded to other network interfaces is not within the scope of the evaluated configuration, and therefore there is no security guarantee associated with them. Outgoing information flow processed with ACL towards other network interfaces is not within the scope of the evaluated configuration,and therefore there is no security guarantee associated with them.

1.4.2.5 Security functionality management

Security functionality management includes not only authentication, administrator role, butalso managing security related data consisting of configuration profile and runtimeparameters. According to security functionality management, customized security isprovided.More functionalities include:

- User management, including user name, passwords, etc.
- Access control management, including the association of users and corresponding privileged functionalities.
- Configure flow control policy.
- Setup to enable/disable SSH or SFTP.
- Routing management, defining IP addresses and address ranges for clients that are allowed to connect to the TOE.

1.4.2.6 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 gainaccess 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 dataand non-TSF data. The following is an enumeration of the subjects and objectsparticipating in the policy.

TSF data:

- User account data, including the following security attributes:
  - User identities.
  - Locally managed passwords.
  - Locally managed administrator role.
- 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 features 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 andfunctions.

1.4.4 Non-TOE hardware and software

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

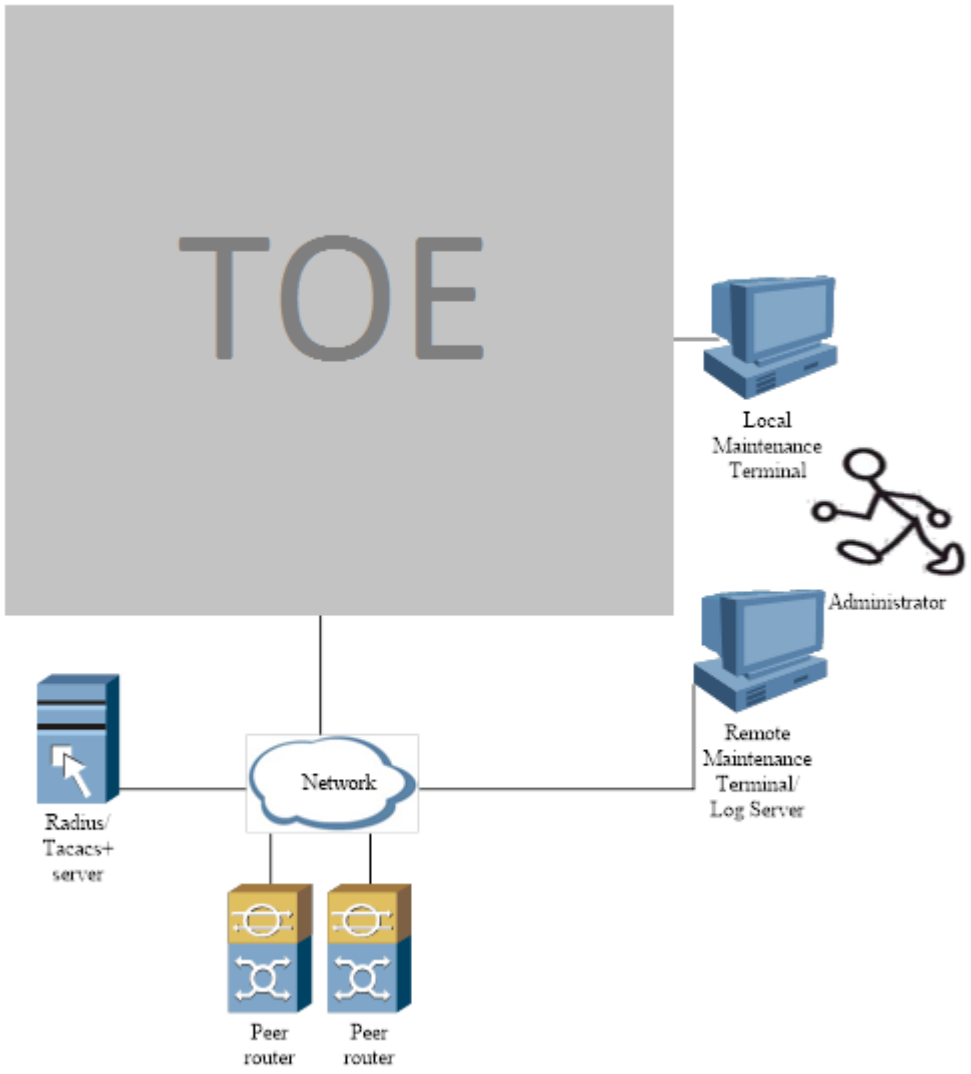

Figure 1-1 TOE boundary and IT environment

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:
  - Generic OS developed later than 2010 (Windows 7/8/8.1/10 or any Linux distribution)
  - Generic Web browser developed later than 2014 with Javascript support.
  - 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:
  - Generic OS developed later than 2010 (Windows 7/8/8.1/10 or any Linux distribution)
  - Generic Web browser developed later than 2014 with Javascript support.
  - 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 TOE and the related environment, physical and logical components of the TOE included inthe evaluation.

1.5.1 Physical scope

Model	**Dimension**	**Picture**
USG6620/6630/6650/6660/6670/6680 Eudemon1000E-N3/N5/N6/N7/N7E	442*470*130.5	
The binary image inside the product is sup.bin which MD5 is cccbf426bc3039844d7d816126e10a56.		

The manual and guides of the productare published at technical support web site (http://www.huawei.com) of Huawei Technologies Co., Ltd.. You can retrieve, browse, and download all the documents online from this site.

- USG6000
    1. Log in to the homepage of Huawei at http://enterprise.huawei.com
    2. If you are not a registered user, you need to go to 3 to register first. If you are already a registered user, go to 4 to log in.
    3. Click Register and register with the system according to the prompt. After the registration succeeds, you will obtain your account and password. Keep them safe.
    4. Enter the user name, password, and displayed verification code, and then click Login.
    5. Click 'Support' button in top of the page. Choose Product Support > Enterprise Networking > Security > NGFW, and click Secospace USG6300, Secospace USG6500.
    6. Download HUAWEI USG6000 Series & NGFW Module V100R001C20SPC100Product Documentation. All the manuals of USG6000 V100R001C20SPC100 are in this compressed package.
- Eudemon200E-N/1000E-N
    1. Log in to the homepage of Huawei at http://support.huawei.com/carrier/
    2. Click "Access Earlier Website".
    3. If you are not a registered user, you need to go to 4 to register first. If you are already a registered user, go to 5 to log in.
    4. Click Register and register with the system according to the prompt. After the registration succeeds, you will obtain your account and password. Keep them safe.
    5. Choose Data Communication > Product > Network Security > Eudemon > Product Manual, and click Eudemon200E-N(V100R001C20SPC100) or Eudemon1000E-N(V100R001C20SPC100).
    6. Download HUAWEI Eudemon200E-N/1000E-N Series & NGFW Module V100R001C20SPC100Product Documentation. All the manuals of Eudemon200E-N/1000E-N V100R001C20SPC100are in this compressed package.

    Notice: The manual documents for carrier products are only available to our technical service employees, carrier customers can get them per request.

The product document includes the following content. (NOTE: The NGFW module is not contained in the TOE scope).

1. Library information

2. Safety and Regulatory Compliance Information
3. Quick Start
4. Product Description
5. Hardware Guide
6. Deployment Guide
7. Administrator Guide
8. Typical Configuration Examples
9. Security Hardening Guide
10. Troubleshooting
11. Reference

1.5.2 Logical Scope

1.5.2.1 Software Architect

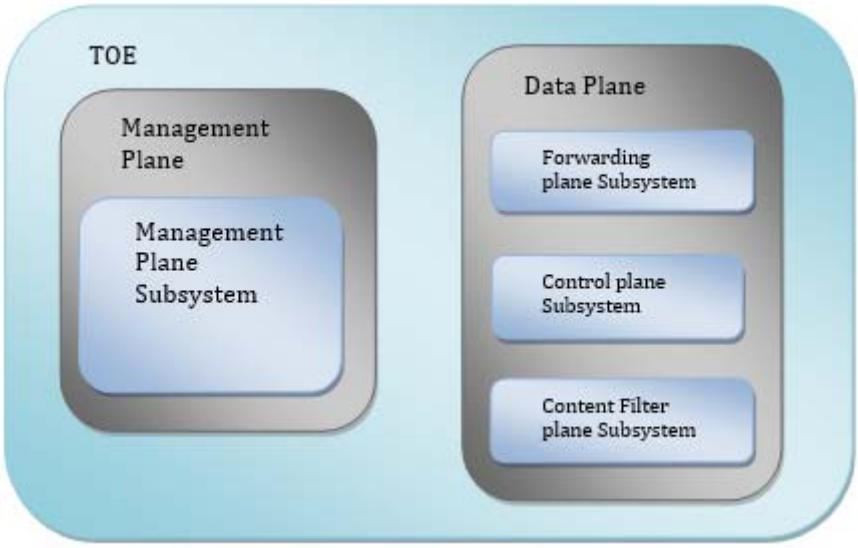

Figure 1-2 Software Architecture of the TOE

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 TOEConfiguration

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

- For management via the console, authentication is always enabled. Authentication mode is password. Length of password for local users is no less than 8 characters
- For management via the ETH interface, authentication is always enabled.
- Service of TELNET and FTP are disabled in this evaluation.
- Authentication of users via RSA when using SSH connections is supported.

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 EAL4+ augmented with ALC_FLR.1.

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, routing configuration data, 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 3-1 Information Assets

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

Table 3-2 lists the threats addressed by the TOE and the IT Environment.

Table 3-2 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 3-3 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 management 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 4-1. 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 4-2. 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 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 the ETH management 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.

4.2.1

4.3 Security Objectives Rationale

Table 4-3. 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).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization).
T.Eavesdrop	The threat of eavesdropping is countered by requiring the communications between the TOE and LMT/RMT, and the other routers/switches and the TOE, are perfomed over a secure channel using SSH, SFTP and HTTPS (O.Communication)

Table 4-4. Rationale for assumptions

Assumption	Rationale for security objectives
A.NetworksElements	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 4-5. 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

There are no extended components defined for this security target.

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.
- Italicized 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 **[20bytes]**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: alluser level assignment;

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:**[**

Subject: users withfollowing security attributes:

a) **user name**
b) **administrator role**
c) **administrator level**

Objects:Configuration andCommands related with specific modules]

Note: The particular users with name “admin” and “audit-admin” are 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 whether the user name matches with the user name of some user built-in. If it does, the TSFgrants this user access to the configuration and commands defined for this user built-in.**

b) **If the user name does not match with any user name built-in, the TSF checks whether the user has some administrator role associated and the Read-Write/Read-Only/None permissions of this role. If it does, the TSF grants this user access to the configuration and commands associated with this administrator role.**

c) **If the user does not have associated any administrator role, the TSF checks whether the user has some administrator level associated. If it does, the user can only execute commands with level lower than or equal to the level assigned to the this user.**

d) **Otherwise, the user can neither execute commands nor access to the configuration.**

¡Error! No se encuentra el origen de la referencia.].

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 **[flow control policy]** on **[**
subjects: external IT entities that send and receiveinformation through the TOE to one another;
information: traffic sent through the TOE from one subject to another;

and
operations: permit ordeny 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 receiveinformation 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 subjectand controlled information via a controlled operation if the following rules hold:**[**
all the information security attributes match the information flow control policy and the action for matched information flow is permit;]

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 ip rfc) &&IP.fragment_offset > 0**

]

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

c) **all the information security attributes match the information flow control policy and the action for matched information flow is deny;**
d) **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 name;**
b) **administrator role;**
c) **administrator level;**
d) **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 behaviuor of***] the functions**[defined in FMT_SMF.1]** to**[the users with system-admin/device-admin rolerefer to 1.4.2.2.1]**.

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 and FIA_ATD.1, except user name**] to [**the users with system-admin rolerefer to 1.4.2.2.1**].

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 [**the users with system-admin/device-admin rolerefer to 1.4.2.2.1]** 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) **user authentication and authorization**
b) **flow control policy**
c) **user management**
d) **SSH**
e) **SFTP**
f) **routing management]**

Note1: The authentication, authorizationare 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 routing 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 [**the users with system-admin/device-admin/device-admin(monitor)/audit-admin rolerefer to 1.4.2.2.1]**

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 4-1.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	This SFRs allows logging out users after an inactivity period.
O.Authorization	FDP_ACC.1	These SFRs ensure that only properly authorized

Objective	SFRs	Rationale
	FDP_ACF.1	admins can access certain functions
	FMT_SMR.1 FIA_ATD.1	These SFRs defines authorization roles and ensure that upon login an administrator gets the proper authorization role.
	FMT_MOF.1 FMT_SMF.1	These SFR lists certain management functions and restricts them to the proper authorization role.
	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 4-2.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 EAL4package 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 4-3.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

Security Functional Requirement	Dependencies	Resolution
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] FCS_CKM.4	FCS_CKM.1/RSA Cryptographic key generation 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, different memory parts is assigned to each process, andthey 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 the Evaluation Assurance Level4+ALC_FLR.1components as specified in [CC] Part 3. No operations are applied to the assurancecomponents.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_FLR.1 Basic flaw remediation
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 4+(ALC_FLR.1 Basic flaw remediation) has been chosen commensurate with the threatenvironment 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 role and administrator level.

(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 two special users built-in. The user name of these users are *admin* and *audit-admin*, and their permissions are predefined.
2. Support 4 built-in administrator roles. This function is achieved by storing corresponding relation in memory.
3. Support user-defined administrator roles. This function is achieved by associating the corresponding configuration/commands related with specific modules.
4. Support assigning administrator role to the users. The TOE requires mandatory username and password specification when a user is created. This function is achieved by associating the corresponding role with the user.
5. Support limiting executing commands of which the role Read-Write/Read-Only/None permission does match with the modules. This function is achieved by performing an check that the permission is matched with the user's role.
6. Support assigning administrator level to the users. The TOE checks whether the administrator user has enough level to execute the required command.

(FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_MOF.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 and SFTP are provided implementing secureTelnet and FTP, to substitute Telnet and FTP which are deemed to haveknown 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 and 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/AES, FCS_COP.1/3DES,FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA, FCS_CKM.1/AES, FCS_CKM.1/3DES,FCS_CKM.1/RSA,FCS_CKM.1/HMAC_SHA)

7.1.4 Flow ControlPolicy

The TOE supports flow controlpolicy 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.

1. Support screening, filtering traffic destined to CPU. This function is achieved by downloading policy configurations into hardware.
2. Support rate limiting traffic based on screened traffic. This function is achieved by downloading configuration of rate into hardware.
3. 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_IFF.1,FDP_IFC.1)

7.1.5 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/RMT clients and the TOE.
- Enabling/disabling SFTP.
- Configure flow control policy.
- Routing management, 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 portbaud rate, data bit, parity, etc;
2. Support configuration for authentication and authorization on user logging in viaconsole port;
3. Support configuration for authentication mode and authorization mode on userlogging in via console port;
4. Support remotely managing the TOE using SSH and HTTPS
5. Support configuration on service port for SSH;
6. Support configuration on RSA key for SSH;
7. Support configuration on authentication type, encryption algorithm for SSH;
8. Support configuration on logout when no operation is performed on the usersession within a given interval;
9. Support management on ARP by specifying static ARP entry, aging time andfrequency of dynamical ARP entry. This function is achieved by interpretingcommands input and storing value in memory.
10. Support management on log by enabling, disabling log output;
11. Support configuration on log output channel, output host;

(FMT_SMF.1, 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/AES,FCS_COP.1/3DES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA,FCS_CKM.1/AES, FCS_CKM.1/3DES,FCS_CKM.1/RSA,FCS_CKM.1/HMAC_SHA).

8 Abbreviations, Terminology and References

8.1 Abbreviations

Acronym	Definition
ACL	Access Control List
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
FTP	File Transfer Protocol
GUI	Graphical User Interface
LMT	Local Maintenance Terminal
MD5	Message-Digest Algorithm 5
RMT	Remote Maintenance Terminal
RSA	Rivest Shamir Adleman
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Functions
VPN	Virtual Private Network
VRP	Versatile Routing Platform

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, unlessstated otherwise.

Administrator: An administrator is a user of the TOE who may have beenassigned specific administrative privileges within the TOE. ThisST may use the term administrator occasionally in an informalcontext, and not in order to refer to a specific role definition -from the TOE's point of view, an administrator is simply a userwho is authorized to perform certain administrative actions onthe 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.

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