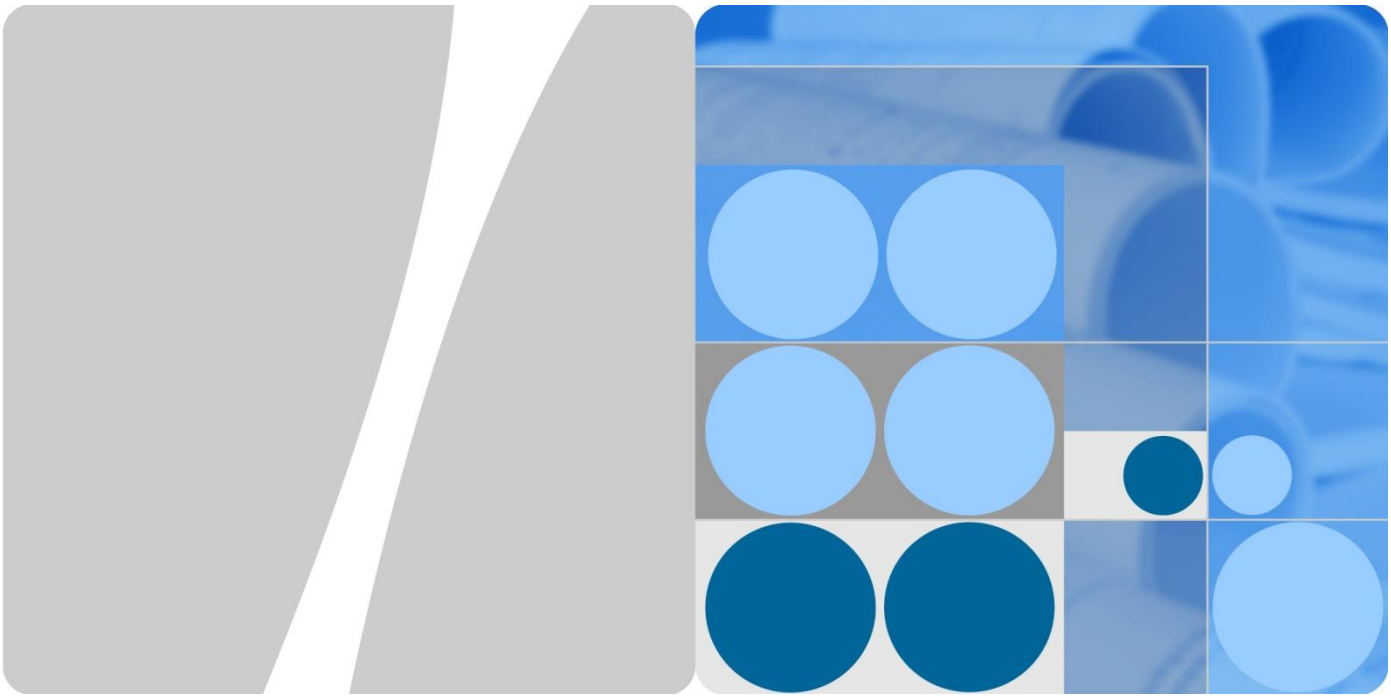


# HUAWEI MA5800 Series Software Management Component V100R020C10 – Security Target

**Issue** 1.1

**Date** 2021-12-06

**HUAWEI TECHNOLOGIES CO., LTD.**

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People’s Republic of China

Website: http://www.huawei.com

# Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

| Date | Version | Change Description | Author |
|---|---|---|---|
| 2021-03-24 | 0.1 | Initial Draft | Yu Hongliang / Brightsight |
| 2021-04-01 | 0.2 | Minor update | Yu Hongliang |
| 2021-04-23 | 0.3 | Minor update | Yu Hongliang |
| 2021-06-02 | 0.4 | Minor update | Zhangchao |
| 2021-10-22 | 1.0 | Minor update | Zhangchao |
| 2021-12-06 | 1.1 | Minor update | Zhangchao |

# Contents

# Figures

# Tables

# 1 Introduction

This Security Target is for the evaluation of MA5800 V100R020C10SPC301 software, consisting of Versatile Routing Platform (VRP). The software is part of MA5800.

## 1.1 ST Identification

**Title:** HUAWEI MA5800 Series Software Management Component V100R020C10SPC301 - Security Target

**Version:** V1.1

**Date:** 2021-12-06

**Author:** Huawei Technologies Co., Ltd.

## 1.2 TOE Identification

**Name:** HUAWEI MA5800 Software Management Component

**Version:** V100R020C10SPC301

**Developer**: Huawei Technologies Co., Ltd.

**Running on Hardware Models:** MA5800-X17, MA5800-X15, MA5800-X7, MA5800-X2

VRC and SPC versions are defined as follows:

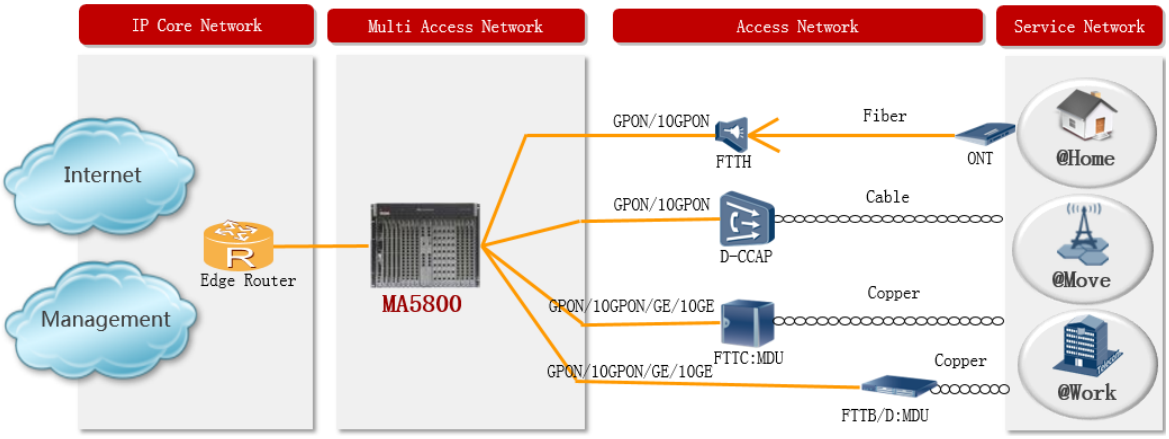
- V version is the version of the software or hardware platform that a product bases.
- R version is released for customer at a specific time. It is a collection of features that is embodied in the form of a product.
- C version is the customized version developed based on the R version to fast meet customer demands.
- SPC version is the cold service patch version of the software.

MA5800 is an OPTICAL multi-service access platform, MA in the model name mean Multi-Access. The TOE is part of the MA5800 software which is the management components of the software running on the MA5800 device. The TOE only consists of the Versatile Routing Platform (VRP) as described in the following chapters and is referred as TOE in this ST.

# 1.3 General product overview

The MA5800 series access nodes including MA5800-X17, MA5800-X15, MA5800-X7 and MA5800-X2, are the aggregation Optical-Line-Terminal (OLT) with a distributed architecture and with different user access interfaces such as Gigabit-capable-Passive-Optical-Network (GPON), 10-Gigabit-capable-Passive-Optical-Network (10G PON), and 10/1G Ethernet (10GE/1GE) protocols. The MA5800 supports deployment on Fiber-To-The-Home (FTTH), Fiber-To-The-Door (FTTD), Fiber-To-The-Building (FTTB), Fiber-To-The-Curb (FTTC), and Distributed-Converged-Cable-Access-Platform (D-CCAP) networks. It functions as a large-capacity aggregation device on the network to aggregate the traffic from Optical-Network-Terminal (ONTs), Multi-Dwelling-Unit (MDUs), and campus switches, thereby simplifying the network architecture and reducing the Operating Expense (OPEX). To the network direction, MA5800s connect to Edge Routers (not a part of TOE) which convert the L2 traffic from MA5800s to L3 IP traffic. The Edge Routers then forward service traffic to Internet Network or management traffic to Management Network. For the position of the MA5800, please refer to Figure 1-1.

**Figure 1-1** Position of the MA5800 on the entire communication network




MA5800 provides several hardware models, including MA5800-X17, MA5800-X15, MA5800-X7, and MA5800-X2. The only difference between these models relies on the service slot quantity (they have the same functions and networks positions). The model ID (e.g. X17) is built according to the following scheme:

- X as first character denotes ‘eXtend’ which means that for this device the number of service boards can be extended.
- The number after the first character denotes the maximum quantity of service boards that can be inserted in this specific chassis.

MA5800 consists of both hardware and software, providing network traffic processing capacity. The TOE is software management component only. Network traffic is processed and forwarded by the underlying hardware according to forwarding rules downloaded from VRP.

The MA5800 runs the VRP developed by Huawei. VRP provides extensive security features, including e.g. different interfaces with according access levels for administrators, enforcing authentications prior to establishment of administrative sessions and auditing of security-relevant management activities.

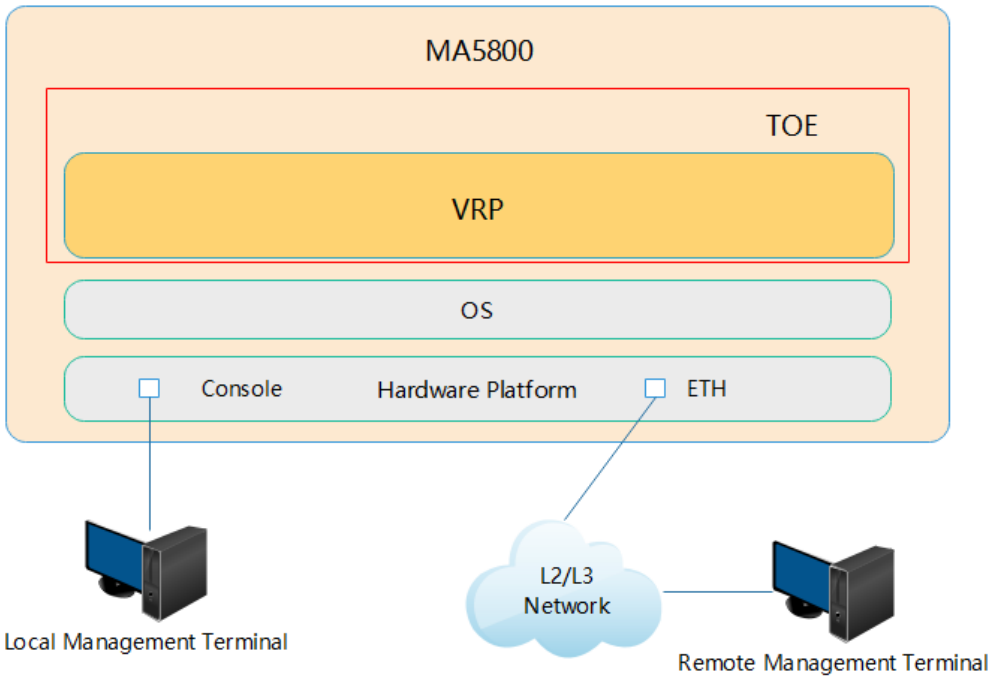
# 1.4 TOE Type and TOE Overview

The MA5800 series devices are optical multi-service access nodes as described in the previous chapter.

The hardware is composed of cabinet, chassis, power unit, and boards. The cabinet is used to install chassis and power units. The power unit is used to supply power to the chassis. The chassis provides the board slot to insert boards. Boards are the core unit of processing and management in the MA5800 series devices. The TOE software is running on the control board of the device, and the TOE is only the management components of the software.

The TOE type is a multi-service access platform (software), which is part of the overall MA5800 software. It consists of the Versatile Routing Platform (VRP) as shown in Figure 1-2, and the TOE consists part of VRP. The underlying operating system contained in the evaluated platforms (RTOS) is not part of the TOE. These components provide the core control and management services of the device.

**Figure 1-2** TOE constitution




The VRP is responsible for managing and controlling the whole MA5800 software, communication, and security features in MA5800. The VRP is relying on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc. The security features of the TOE are all provided by the VRP.

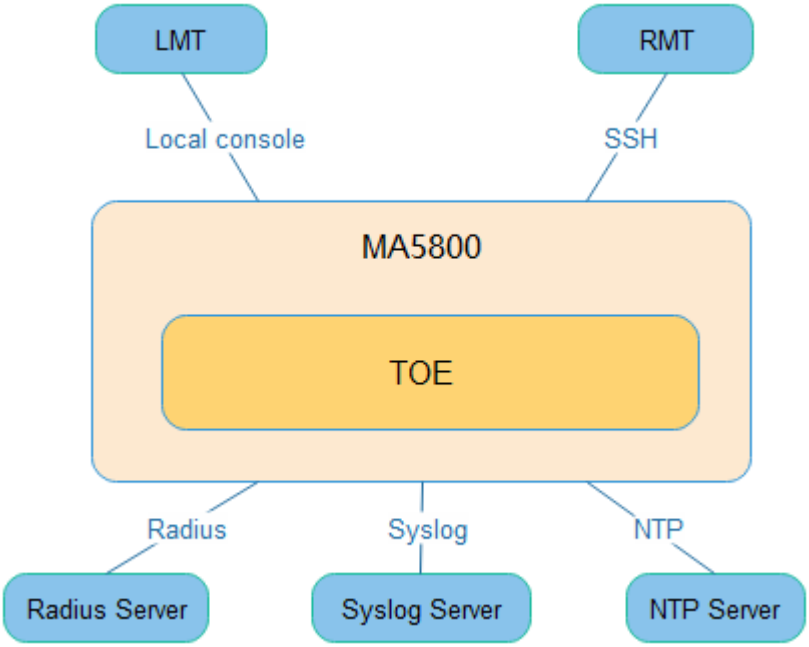
To counter the security threats of MA5800, the VRP provides security measures to mitigate security risks effectively. The main security features are:

1. Identification and authentication of administrative users
2. Authorization
3. Auditing
4. Communication security
5. Management traffic flow control
6. Security functionality management

The detailed description of the security features above is in the chap.1.5.

The TOE provides all the security functions. The external entities which may communicate with the TOE and the protocol used between them are shown in Figure 1-3.

**Figure 1-3** External entities communicate with the TOE




The CLI interface of the TOE can be accessed either through LMT (Local Maintenance Terminal) via the Console port on the control board or through RMT (Remote Maintenance Terminal) via a secure SSHv2 channel via the ETH port on the control board.

The TOE supports authenticating the username and password locally from local database, or remotely in AAA (Authentication, Authorization, and Accounting) server using RADIUS protocol.

The TOE supports report audit information to SYSLOG Server.

The TOE supports synchronizing time from NTP server.

# 1.5 TOE description

## 1.5.1 Physical scope

The TOE is software only (software package version: V100R020C10) and is limited to the management components of the software. It is running on MA5800-X17, MA5800-X15, MA5800-X7 and MA5800-X2 devices. The hardware and the firmware are out of the TOE scope. The firmware contains the driver software necessary to communicate with the hardware as well as the software that is needed to load the TOE software onto the device after delivery to the user. The devices with firmware are shipped in sealed boxes through worldwide logistics service providers to regional warehouses, from where the devices are delivered to customers efficiently and securely. The TOE software as well as the guidance documents as pdf files need to be downloaded by the user through Huawei's support website and the user has to verify the signature values for all TOE parts for secure acceptance.

**Table 1-1 TOE List**

| Type | Delivery Item | Version |
|---|---|---|
| **Software** | MA5800 V100R020C10 Software for MPLx/MPSA control boards:<br>MA5800V100R020C10SPC301.zip | V100R020C10 SPC301 |
| **Software Signature File** | MA5800V100R020C10SPC301.zip.asc | V100R020C10 SPC301 |
| **Product Guidance** | SmartAX MA5800 Product Documentation<br>Note:<br>Users can login the HUAWEI support website to read the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website. | Issue 02 |
| | Huawei MA5800 Series V100R020C10SPC301 Software – Preparative Procedures | V1.0 |
| | Huawei MA5800 Series V100R020C10SPC301 Software - Operational User Guidance | V1.0 |
| | Huawei MA5800 Series V100R020C10SPC301 Software - Configuration and Reference | V1.0 |

# 1.5.2 Logical Scope

## 1.5.2.1 Authentication

The CLI interface of the TOE can be accessed either through LMT (i.e. the ‘console’) or RMT (i.e. via virtual terminals, ‘VTYs’). The LMT can only access the TOE via the console port of the TOE, it is authenticated by username and password. The RMT accesses the TOE via SSH, and is authenticated by username and password or public key, and the authentication modes include password only, public key only, password and public key, password or public key. Only authenticated users can execute commands of the TOE. The password policy requires 12 characters at least and the password can be composed of uppercase letters, lowercase letters, numbers and special characters, the password must contain at least one uppercase letter, one lowercase letter, one number and one special character.

The TOE provides a local authentication mode, or can optionally enforce authentication decisions obtained from an AAA server in the IT environment.

In local authentication mode, accounts and passwords are saved on the local equipment and authenticated using the local account and password by the local equipment during login. In remote authentication mode, accounts and passwords are saved on the AAA server and authenticated by the AAA server. During login, the accounts and passwords are forwarded to the AAA server, using the RADIUS protocol and the AAA server checks the validity of accounts and passwords.

User authentication is always enforced for virtual terminal sessions via SSH sessions and local terminal session via the console. The use of SSH connection is always required for accessing the TOE via RMT. For LMT no logically secured communication channel is required.

## 1.5.2.2 Authorization

Authorization indicates that devices assign operation authorities to accounts according to their validity.

The TOE manages user privileges by access level. There are in total 3 hierarchical access levels ranging from 0 ~ 2. The bigger the number, the higher is the privilege. Correspondingly, levels from 0~2 can be assigned to all commands provided by the TOE. A user can access a command if the command's access level is lower or equal to the user's access level. By default, commands are registered with level 0~2.

The 3 hierarchical access control levels are reflected by the following table.

**Table 1-2** Access Levels

| User level | Level name | Authority |
|---|---|---|
| 0 | Common user | Perform basic system operations and simple query operations. |
| 1 | Operator | Perform basic configuration operations for the service and device. |
| 2 | Administrator | Perform all configuration operations. Maintain and manage the device, perform security management, create other user including administrator, operator and common user accounts. |

All authenticated users with an access level equal or higher to the access level of the command (also referred to as 'command level') are allowed to execute the corresponding command.

### 1.5.2.3 Auditing

The TOE generates audit records for security-relevant management actions. All audit records contain not only the information on the event itself but also a timestamp and – if applicable – additional information like user ID, source IP, etc.

Audit functionality is activated by default and cannot be deactivated.

The TOE supports writing the audit records in local storage or sending the audit records to external audit servers via SYSLOG protocol. When writing into the local storage, audit records are written into log buffer first and then transported to log files in Flash.

### 1.5.2.4 Communication Security

The TOE provides communication security by implementing the SSHv2 protocol. The TOE can act as both STELNET server and STELNET client. When the RMT accesses the TOE, the TOE acts as STELNET server, and when the users who login the TOE access other SSH server via STELNET, the TOE acts as STELNET client.

To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSHv2 provides:

- Authentication of client by password or RSA public key;
- AES encryption algorithms;
- HMAC integrity verification algorithms;
- Secure cryptographic key exchange.

The TOE does not offer cryptographic services, but uses cryptographic mechanisms in the implementation of its communication security functions (SSH) and I&A functions (SSH public key authentication). The TOE is capable of generating the necessary keys (AES, RSA).

### 1.5.2.5 Management Traffic Flow Control

For administration of the TOE, network packages have to be sent to the TOE from the management network. When a network packet reaches the TOE from the management network, the TOE applies an information flow security policy in the form of Access Control Lists (ACLs) to the traffic before processing it. Network packets on Layer 3 from the management network arriving at a network interface of the TOE are checked to ensure that they conform to the configured packet filter policy. Packet flows matching a deny rule in the ACL are dropped. If no rule is specified for an incoming packet, it is forwarded by default. Through this the TOE provides network filtering based on ACLs for the management network as a security function.

Users with sufficient access rights can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection-oriented or connectionless packets against ACL rules specified. Ethernet protocol type, 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, etc., can be used for ACL rule configuration.

### 1.5.2.6 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:

- Management of user accounts and user attributes, including user credentials.
- Management of authentication failure policy.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling and disabling trusted channels for local and remote access to the TOE's management interfaces.
- Management of ACLs and ACL attributes and parameters like IP addresses or address ranges.
- Configuration of network addresses for services used by the TOE, like NTP, SYSLOG, SSH.
- Management of the TOE's time.

All security management functions (i.e. commands related to security management) require sufficient user level for execution.

## 1.5.3 Non-TOE Hardware and Software

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

- For CLI management via the console, authentication is always enabled. Authentication mode is username and password or Authentication, Authorization, Accounting ('AAA', i.e. username and password). Length of password is no less than 8 characters.
- For CLI management via the ETH interface, the SSH protocol must be used, and authentication is always enabled. Authentication mode is password, public key or Authentication, Authorization, Accounting ('AAA', i.e. username and password). Length of password is no less than 8 characters.

The environment for TOE comprises the following components:

- Local PCs used by administrators to connect to the TOE for access of the command line interface either through TOE's console interface or TOE's ETH interface via a secure channel enforcing SSH.
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through ETH interfaces within the TOE via a secure channel enforcing SSH.
- Radius server is optional and is used for centralized authentication via Radius protocol.
- Syslog server is optional and is used for receiving audit information from the TOE via SYSLOG protocol.
- NTP server is used for synchronizing time to the TOE.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- MA5800 hardware, firmware and non-TOE software, including BIOS/OS/FPGA/CPLD of the control board.
- The hardware of the control boards of MA5800 are non-TOE components, the control boards include the following types:
    - H901MPLA
    - H902MPLA
    - H903MPLA
    - H901MPLB
    - H902MPLB
    - H901MPSA-G

# 2 CC conformance claims

## 2.1 CC Conformance Claim

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

The ST claims conformance to the EAL4 augmented with ALC_FLR.2.

No conformance to a Protection Profile is claimed.

# 3 Security Problem Definition

## 3.1 Assets

The assets to be protected are the information stored, processed or generated by the TOE. Including below:

1. Audit data: The data which is provided by the TOE during security audit logging
2. Authentication data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
3. Crypto data: All data used by the TOE for cryptographic operations like digital signature handling and encryption or decryption purposes. This includes symmetric and asymmetric cryptographic keys.
4. Configuration data for the TOE, which is used for configuration of security features and functions
5. Management Traffic data, which is the management information exchanged between the TOE and the LMT/RMT from authorized users.

## 3.2 Threats

This section specifies the threats that are addressed by the TOE and the TOE environment.

As a result, the following threats have been identified:

### 3.2.1 Threats

**T.UnwantedManagementTraffic** The traffic here only refers to the traffic on management interfaces, which means, the Unwanted Network Traffic threat only exists on the management plane. The Unwanted network traffic may originate from an attacker and result in an overload of the management interfaces, which may cause a failure of the TOE to respond to system control and normal management operations. As a consequence, the TOE might be unable to provide some of the TSF while under attack and in particular security management functionality to update configuration data for the TOE. Subsequently, backup of audit information before local storage space is exceeded and old audit information is overwritten by new audit events could be affected. Therefore, Audit data and Configuration data for the TOE are assets that could be affected by this threat, too.

**T.UnauthenticatedAccess** An unauthenticated person may attempt to bypass the security of the TOE so as to access the TOE. This could affect all assets as defined in chap. 3.1.

**T.UnauthorizedAccess** A user with restricted action and information access authorization gains access to unauthorized commands or information. This threat also includes data leakage to non-intended person or device. This could affect all assets as defined in chap. 3.1.

**T.Intercept** A remote attacker is able to intercept, modify and re-use management information assets that are exchanged between the TOE and RMT. This comprises Authentication data (in particular

authentication data of administrative users), Crypto data (regarding this threat mainly data related to session keys used for secure communication), and Configuration Data for the TOE. All these assets could be affected by this threat.

### 3.2.2 Threats Components

- **T.UnwantedManagementTraffic**
  **Threat agent:** Attacker.
  **Asset:** Audit data, Configuration data.
  **Adverse action:** Disturbance on TOE operation.

- **T.UnauthenticatedAccess**
  **Threat agent:** Unauthenticated person.
  **Asset:** Authentication data, Audit data, Configuration data, Crypto data, Management Traffic data.
  **Adverse action:** Access to the TOE.

- **T.UnauthorizedAccess**
  **Threat agent:** User with restricted action and information access authorization.
  **Asset:** Authentication data, Audit data, Configuration data, Crypto data, Management Traffic data.
  **Adverse action:** Access to unauthorized commands or information.

- **T.Intercept**
  **Threat agent:** Remote attacker in the management network.
  **Asset:** Authentication data, Crypto data, Configuration data.
  **Adverse action:** Intercept, modify and re-use management information assets that are exchanged between the TOE and RMT.

## 3.3 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

**A.PhysicalProtection** It is assumed that the TOE and its operational environment (i.e. the complete system including attached peripherals) are protected against unauthorized physical access. It is assumed that only administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) with explicit approval by the administrator(s) are authorized to physically access the TOE and its operational environment. This assumption includes that the local management network, including the AAA server (RADIUS server), SYSLOG server, NTP server and locally attached management terminals (LMT) together with all related communication lines are operated in the same physically secured environment as the TOE. Remote management terminal (RMT) needs to be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic means and do not need any physical protection. It is assumed that all RMT as well as peripherals like AAA server, NTP server or SYSLOG server are connected to the TOE via the same segregated management network (see also A.NetworkSegregation).

**A.NetworkElements** It is assumed that the operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. These network devices are

deployed in an independent network which is segregated from other network by VPN or firewall or other methods. Examples of such devices are:

- Peer router(s) for the exchange of dynamic routing information;
- Local and remote management terminals (LMTs, RMTs) used for administration of the TOE.
- RADIUS servers for obtaining authentication and authorization decisions.
- SYSLOG servers for receiving and storing audit data.
- NTP servers.

**A.NetworkSegregation** It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.

**A.NoEvil** It is assumed that personnel working as authorized administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

**A.Device** It is assumed that the underlying hardware of MA5800, which is outside the scope of the TOE, as well as the firmware and the underlying OS and non-TOE software, work correctly.

**A.UpToDateClient** It is assumed that the user uses a secure remote management terminal for remote administration of the TOE which is up to date with respect to supported cryptographic algorithms and security measures.

# 4 Security Objectives

## 4.1 Security Objectives for TOE

The following objectives must be met by the TOE:

- **O.DataFilter** The TOE shall ensure that only allowed management traffic goes through the TOE.
- **O.Authorization** The TOE shall implement different authorization roles that can be assigned to users in order to restrict the functionality that is available to them.
- **O.Authentication** The TOE shall authenticate the user before access to the data and security functions is granted. If the user accesses the TOE through an RMT, the TOE shall allow establishment of a secure remote session to the TOE prior to user authentication.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrator actions and user log in and log out activities.
- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and RMT from the operational environment.
- **O.SecurityManagement** The TOE shall provide functionality to manage security functions provided by the TOE.

## 4.2 Security Objectives for the Operational Environment

- **OE.PhysicalProtection** The TOE and its operational environment (i.e. the complete system including attached peripherals) shall be protected against unauthorized physical access. Only administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) with explicit approval by the administrator(s) shall be authorized to physically access the TOE and its operational environment. The local management network, including the RADIUS server, SYSLOG server, NTP server and locally attached management terminals (LMT) together with all related communication lines shall be operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) shall be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic means and do not need any physically protection. All RMTs as well as peripherals like AAA server, NTP server or SYSLOG server shall be connected to the TOE via the same segregated management network (see also OE.NetworkSegregation). As a result, the TOE and its operational environment shall be physically protected and shall not be subject to physical attacks.

**OE.NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. The behavior of such network devices provided by the operational environment shall be secure and correct. Examples of such devices are:

- Peer router(s) for the exchange of dynamic routing information;
- Local and remote management terminals (LMTs, RMTs) used for administration of the TOE.
- RADIUS servers for obtaining authentication and authorization decisions.
- SYSLOG servers for receiving and storing audit data.
- NTP servers for synchronizing time to the TOE.

- **OE.NetworkSegregation** The operational environment shall provide segregation of networks by deploying the management interface in TOE into an independent local network.
- **OE.NoEvil** Personnel working as authorized administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users shall be competent, and not careless or willfully negligent or hostile, and shall follow and abide by the instructions provided by the TOE documentation.
- **OE.Device** The underlying hardware of MA5800, which is outside the scope of the TOE, as well as the firmware and the underlying OS and non-TOE software, shall work correctly.
- **OE.UpToDateClient** The user shall use a secure remote management terminal for remote administration of the TOE which is up to date with respect to supported cryptographic algorithms and security measures.

# 4.3 Rationale for Security Objectives

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

**Table 4-1** Mapping objectives to threats and OSPs

| Threat / OSP | Security Objectives | Rationale for Security Objectives |
|---|---|---|
| T.UnwantedManagementTraffic | O.DataFilter<br>O.SecurityManagement<br>OE.NetworkSegregation | This threat is countered by O.DataFilter ensuring that unwanted traffic is filtered and cannot deplete the network resources.<br>The filter rules can be configured by authorized users with sufficient user level (O.SecurityManagement).<br>An independent local network is used to manage the TOE.<br>(OE.NetworkSegregation) |

| Threat / OSP | Security Objectives | Rationale for Security Objectives |
|---|---|---|
| T.UnauthenticatedAccess | O.Authentication<br>O.Audit<br>O.SecurityManagement | The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication).<br>Authentication mechanisms can be configured by users with sufficient user level (O.SecurityManagement). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit). |
| T.UnauthorizedAccess | O.Authorization<br>O.Audit<br>O.SecurityManagement | The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization).<br>Access control mechanisms (including user levels) can be configured by users with sufficient user level (O.SecurityManagement).<br>In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit). |
| T.Intercept | O.Communication<br>O.SecurityManagement | The threat of eavesdropping is countered by requiring communications security via SSH for communication between RMT and the TOE (O.Communication).<br>Management of secure communication channels can be performed by users with sufficient user level (O.SecurityManagement). |

The following table provides a mapping of the objectives for the operational environment to assumptions, showing that each objective is covered exactly by one assumption. The objectives for the environment are mirrored by the assumptions. Therefore, the mapping is trivial.

**Table 4-2** Mapping objectives for the environment to assumptions

| Environmental Objective | Threat / Assumption |
|---|---|
| OE.PhysicalProtection | A.PhysicalProtection |
| OE.NetworkElements | A.NetworkElements |
| OE.NetworkSegregation | A.NetworkSegregation<br>T.UnwantedManagementTraffic |
| OE.NoEvil | A.NoEvil |

| | |
|---|---|
| OE.Device | A.Device |
| OE.UpToDateClient | A.UpToDateClient |

# 5 Security Functional Requirements

## 5.1 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/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

## 5.2 Functional Security Requirements

### 5.2.1 Security Audit (FAU)

#### 5.2.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***not specified*** level of audit; and

**c) The following auditable events:**

**i. user activity**

**1) login, logout**

**ii. management of user accounts**

**1) add, delete, modify (including change of user level)**

**2) password change (by the user himself)**

**3) session termination**

**iii. authentication policy modification**

**iv. system management**

**1) operation requests (i.e. configuration of the device after start-up)**

**v. log management**

**1) log policy modification**

Application Note: Audit functionality is enabled by default during start-up of the device and cannot be disabled.

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

a) Date and time of the event, type of event (if applicable), subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **IP address (if applicable)**, **User ID (if applicable), and CLI command name (if applicable).**

## 5.2.1.2 FAU_GEN.2 User identity association

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

## 5.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **administrators** with the capability to read **all information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

## 5.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **selection** of audit data based on **log level, size and time scope.**

## 5.2.1.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***prevent*** unauthorized modifications to the stored audit records in the audit trail.

## 5.2.1.6 FAU_STG.3 Action in case of possible audit data loss

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

Application Note: The audit records are stored in one uncompressed file (which name is log.log) and several compressed files. The size of the log.log is configurable by the administrator with value 4M/8M/16M/32M bytes, and by default is 8MB. When the size of log.log exceeds the configured maximum size, the log.log is compressed into a smaller ZIP file. The storage space for log.log and compressed log file in flash is about 14M, and when the storage space occupancy exceeds 70%, the system deletes oldest compressed files to save the latest compressed log file.

## 5.2.2 User Data Protection (FDP)

### 5.2.2.1 FDP_ACC.1 Subset Access Control

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

**Subject: users;**

**Objects: commands provided by TOE;**

**Operation: execute**

### 5.2.2.2 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 security attributes:**

**Users and their following security attributes:**

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

**Objects security attributes:**

**Commands and their following security attributes:**

- **Command level**

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

1) **Only authorized users are permitted access to commands.**
2) **Users can be configured with different user levels to control the device access permission.**
3) **There are 3 user access levels and command levels numbered from 0-2.**
4) **A user can access a command if the command's access level is lower or equal to the user's access level.**
5) **The command level is stored by the TOE (i.e. by the VRP software) and can be modified by the administrator.**

FDP_ACF.1.3 The TSF shall explicitly authorize 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**

### 5.2.2.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the **Management Network Filtering SFP** on

**Subjects:**

- **Device management interface**

**Information:**

- **IP packets**

**Operations:**

- **Device management interface will accept or deny IP packets based on the settings of the device management interface and the IP packets content (i.e. subject attributes and information security attributes as defined in 5.2.2.4 ).**

### 5.2.2.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **Management Network Filtering SFP** based on the following types of subject and information security attributes

**Subject:**

- **Device management interface**

**Subject attributes:**

- **IP address (i.e. IP address setting of the device management interface)**
- **Port number**

**Information security attributes:**

- **Source IP address**
- **Destination IP address**
- **IP Protocol number**
- **Source port number**
- **Destination port number**

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:

1) **The TOE uses the Access Control List (ACL) to match the IP packets received from the device management interface. If the IP packet match an ACL rule, the TOE discards or accepts the packets based on the action specified in the ACL rule.**
2) **An ACL rule contains one or more of the following attributes: source IP address, destination IP address, IP protocol number, source port number, and destination port number.**

FDP_IFF.1.3 The TSF shall enforce the **no additional information flow control SFP rules**.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **none.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **none.**

# 5.2.3 Identification and Authentication (FIA)

## 5.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **the last successful authentication of the indicated user identity**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **terminate the session of the user trying to authenticate and block the user account and IP address for authentication for at least 15 minutes**.

## 5.2.3.2 FIA_ATD.1 User Attribute Definition

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

1) **User ID**
2) **User level**
3) **User password**
4) **User public key**
5) **The inactivity time after which an account is automatically logged out.**
6) **Status of the account (locked/unlocked)**

## 5.2.3.3 FIA_UAU.1 Timing of authentication

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

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

## 5.2.3.4 FIA_UAU.5 Multiple Authentication Mechanisms

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

1) **Remote authentication by RADIUS for authentication via RMT**
2) **Local Authentication by local database of the TOE for authentication via LMT and RMT**

to support user authentication.

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

1) **For Remote authentication by RADIUS for authentication via RMT**
2) **For local authentication, the TSF authenticates the users based on the configured Identification (including user id and password for authentication via LMT and RMT or public key for authentication via RMT).**

Application Note: The TOE can use only one of the mechanisms at any given time. The administrator can configure which mechanism is used by the TOE.

### 5.2.3.5 FIA_UID.1 Timing of identification

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

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

## 5.2.4 Security Management (FMT)

### 5.2.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine the behavior*** of the functions **identified in FMT_SMF.1** to **users with administrator user level as defined in FMT_SMR.1.**

Application Note: Access control of the TOE works as follows: Users can only execute a command if their associated user level is equal or higher compared to the command level.

### 5.2.4.2 FMT_MSA.1/ACFATD Management of security attributes

FMT_MSA.1.1/ACFATD The TSF shall enforce the **access control policy** to restrict the ability to ***query, modify*** the security attributes **identified in FDP_ACF.1 and FIA_ATD.1** to **users with administrator user level as defined in FMT_SMR.1**.

Application Note: See Application Note for FMT_MOF.1 for clarification.

### 5.2.4.3 FMT_MSA.1/IFF Management of security attributes

FMT_MSA.1.1/IFF The TSF shall enforce the **Management Network Filtering SFP (based on ACL)** to restrict the ability to ***modify, delete*** the security attributes **identified in FDP_IFF.1** to **users with administrator or operator user level as defined in FMT_SMR.1.**

### 5.2.4.4 FMT_MSA.3/ACFATD Static attribute initialization

FMT_MSA.3.1/ACFATD The TSF shall enforce the **access control policy** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ACFATD The TSF shall allow **users with administrator user level as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

### 5.2.4.5 FMT_MSA.3/IFF Static attribute initialization

FMT_MSA.3.1/IFF The TSF shall enforce the **Management Network Filtering SFP (based on ACL)** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/IFF The TSF shall allow **users with administrator or operator user level as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

### 5.2.4.6 FMT_SMF.1 Specification of Management Functions

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

1) **Management of user accounts and user attributes, including user credentials**
2) **Management of authentication failure policy**
3) **Management of ACLs and ACL parameters like IP addresses or address ranges**
4) **Configuration of network addresses for services used by the TOE, like NTP, SYSLOG, and RADIUS etc.**
5) **Enabling/disabling trusted channels for remote access to the TOE's management interfaces**
6) **Management of the TOE's time**
7) **Management of command levels**

### 5.2.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

1) **Administrator: Perform all configuration operations. Maintain and manage the device, perform security management, create other users including administrator, operator and common user accounts.**
2) **Operator: Perform basic configuration operations for the service and device.**
3) **Common User: Perform basic system operations and simple query operations.**

Application Note: The roles are hierarchical, i.e. each role includes all authorities of the previous roles in addition to the authorities described for the role itself.

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

## 5.2.5 TOE Access (FTA)

### 5.2.5.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1: The TSF shall terminate an interactive session after a **time interval of session inactivity of 5 minutes**.

Application Note: The time interval of session inactivity is 5 minutes by default and the administrator shall not change this time interval.

### 5.2.5.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

1) **User authentication failure (password and/or public key authentication failure)**

**2) Source IP address (applies to remote administration only)**

# 5.2.6 Trusted path/channels (FTP)

## 5.2.6.1 FTP_TRP.1/SSH Trusted Path

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

FTP_TRP.1.2/SSH The TSF shall permit ***the TSF and remote users*** to initiate communication via the trusted path.

FTP_TRP.1.3/SSH The TSF shall require the use of the trusted path for ***initial user authentication and remote management.***

Application Note: To establish a trusted path, the SSH protocol shall be used that complies with RFCs 4344 [RFC4344], 4251 [RFC 4251], 4252 [RFC 4252], 4253 [RFC 4253], 4254 [RFC 4254], 5647 [RFC 5647], 6668 [RFC 6668] and 8332 [RFC8332]. The TOE acts as both STELNET server and STELNET client. For SSH-based communication the following algorithms are supported.

- Client authentication can be performed either public key-based or password-based as described in [RFC 4252].
- Key exchange is performed using diffie-hellman-group-exchange-sha256
- The public key algorithm of the SSH transport implementation is rsa-sha2-256 and rsa-sha2-512.
- For data encryption AES128-CTR, AES192-CTR, AES256-CTR, AES256-GCM and AES128-GCM are supported.
- For data integrity protection HMAC-SHA512 and HMAC-SHA256 are supported.

# 5.3 Security Functional Requirements Rationale

# 5.3.1 Coverage

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements:

**Table 5-1** Mapping SFRs to objectives

| Security Functional Requirements | Objectives |
|---|---|
| FAU_GEN.1 | O.Audit |
| FAU_GEN.2 | O.Audit |
| FAU_SAR.1 | O.Audit |
| FAU_SAR.3 | O.Audit |

| | |
|---|---|
| FAU_STG.1 | O.Audit |
| FAU_STG.3 | O.Audit |
| FDP_ACC.1 | O.Authorization |
| FDP_ACF.1 | O.Authorization |
| FDP_IFC.1 | O.DataFilter |
| FDP_IFF.1 | O.DataFilter |
| FIA_AFL.1 | O.Authentication |
| FIA_ATD.1 | O.Authentication<br>O.Authorization |
| FIA_UAU.1 | O.Authentication |
| FIA_UAU.5 | O.Authentication |
| FIA_UID.1 | O.Authentication<br>O.Authorization |
| FMT_MOF.1 | O.Authorization<br>O.SecurityManagement |
| FMT_MSA.1/ACFATD | O.Authorization<br>O.SecurityManagement |
| FMT_MSA.1/IFF | O.DataFilter<br>O.SecurityManagement |
| FMT_MSA.3/ACFATD | O.Authorization<br>O.SecurityManagement |
| FMT_MSA.3/IFF | O.DataFilter<br>O.SecurityManagement |
| FMT_SMF.1 | O.SecurityManagement<br>O.DataFilter |
| FMT_SMR.1 | O.Authorization<br>O.SecurityManagement |
| FTA_SSL.3 | O.Authentication<br>O.Communication |
| FTA_TSE.1 | O.DataFilter<br>O.Authentication<br>O.Communication |
| FTP_TRP.1/SSH | O.Authentication |

| | |
|---|---|
| | O.Communication |

## 5.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

**Table 5-2** SFR sufficiency analysis

| Security objective | Rationale |
|---|---|
| O.DataFilter | The requirement of ACL is defined in FDP_IFF.1 and FDP_IFC.1 and the impact on session establishment is covered in FTA_TSE.1. The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/IFF, FMT_MSA.3/IFF and FMT_SMF.1. |
| O.Audit | The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by the external NTP server and user identities as defined in FAU_GEN.2 where applicable.<br>Requirements on reading audit records are defined in FAU_SAR.1 and FAU_SAR.3. The protection of the stored audit records against unauthorized modification is implemented in FAU_STG.1. If the audit trail exceeds the size of the storage device The TSF shall roll back the oldest records as required by FAU_STG.3. |
| O.Communication | Communication security is implemented by the establishment of a trusted path in FTP_TRP.1/SSH. Termination of inactive SSH sessions is covered by FTA_SSL.3. FTA_TSE.1 addresses that session establishment is denied if an ACL exists that specifies a deny rule for the attempted connection. |
| O.Authentication | User authentication is implemented by FIA_UAU.1, and FIA_UAU.5, supported by individual user identification in FIA_UID.1. The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1.<br>Client authentication for SSH sessions is covered by FTP_TRP.1/SSH. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1. |
| O.Authorization | User identification is addressed in FIA_UID.1. The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. User-related attributes are spelled out in FIA_ATD.1.<br>Access control is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1 and FMT_MOF.1. Requirements on the management functionality for the definition of access control policies are provided in FMT_MSA.1/ACFATD and FMT_MSA.3/ACFATD. |

| | |
|---|---|
| O.Security Management | The management functionality for the security functions of the TOE is defined in FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD and FMT_MSA.3/IFF and the security user roles are defined in FMT_SMR.1. |

## 5.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL4 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again. The augmentation by ALC_FLR.2 does not cause any additional dependencies.

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

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

**Table 5-3** Dependencies between TOE security functional requirements

| Security Functional Requirement | Dependency | Resolution |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | This TOE relies on the external NTP server to provide the timestamp and it does not provide the reliable timer. |
| FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.1 | FAU_GEN.1<br>FIA_UID.1 |
| FAU_SAR.1 | FAU_GEN.1 | FAU_GEN.1 |
| FAU_SAR.3 | FAU_SAR.1 | FAU_SAR.1 |
| FAU_STG.1 | FAU_GEN.1 | FAU_GEN.1 |
| FAU_STG.3 | FAU_STG.1 | FAU_STG.1 |
| FDP_ACC.1 | FDP_ACF.1 | FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | FDP_ACC.1<br>FMT_MSA.3/ACFATD |
| FDP_IFC.1 | FDP_IFF.1 | FDP_IFF.1 |
| FDP_IFF.1 | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1<br>FMT_MSA.3/IFF |
| FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.1 |
| FIA_ATD.1 | No Dependencies | None |
| FIA_UAU.1 | FIA_UID.1 | FIA_UID.1 |

| Security Functional Requirement | Dependency | Resolution |
|---|---|---|
| FIA_UAU.5 | No Dependencies | None |
| FIA_UID.1 | No Dependencies | None |
| FMT_MOF.1 | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| FMT_MSA.1/ACFATD | [FDP_ACC.1, or FDP_ICF.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_ACC.1<br>FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MSA.1/IFF | [FDP_ACC.1, or FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_IFC.1<br>FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MSA.3/ACFATD | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1/ACFATD<br>FMT_SMR.1 |
| FMT_MSA.3/IFF | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1/IFF<br>FMT_SMR.1 |
| FMT_SMF.1 | No Dependencies | None |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.1 |
| FTA_SSL.3 | No Dependencies | None |
| FTA_TSE.1 | No Dependencies | None |
| FTP_TRP.1/SSH | No Dependencies | None |

# 5.4 Security Assurance Requirements

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

# 5.5 Security Assurance Requirements Rationale

The evaluation assurance level 3 augmented with ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL package selected (EAL4 augmented with ALC_FLR.2) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here.

# 6 TOE Summary Specification

## 6.1 Authentication

The TOE can identify users by a unique ID and enforces their authentication before granting them access to CLI interface. Detailed functions include:

1) The TOE supports user authentication via username and password. This function is achieved by comparing user information input with reference values stored in memory.
2) The TOE supports user authentication via remote RADIUS authentication server. This function is achieved by performing pass/fail action based on result from remote authentication server.
3) The TOE supports user authentication using SSH by password, RSA public key or combination of password and RSA public key. For this the TSF associate the security attributes User ID and User level with subjects acting on behalf of that user.
4) The TOE stores the following security attributes for individual users:
   - User ID
   - User level
   - User password
   - User public key
   - The inactivity time after which an account is automatically logged out
   - Status of the account (locked/unlocked)
   - Number of failed authentication attempts within a certain period of time and timestamp of last successful login
5) The TOE locks out an account or corresponding IP address if the number of login failures meets the number of 3 unsuccessful login attempts. The TOE will prevent the locked account and IP address from login into the system until the locking out time period of at least 15 minutes has elapsed.
6) The TOE requires the user to be successfully authenticated before he can perform any other TSF-mediated actions when connecting to the TOE. If the user accesses the TOE through an RMT, the user must establish a secure remote session to the TOE prior to user authentication.
7) The TOE supports limiting the access to CLI interface by IP whitelist or blacklist, or by ACL policy.
8) The TOE support logout when no operation is performed on the user session within a given interval of 5 minutes.

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

# 6.2 Authorization

The TOE enforces an access control by supporting following functionalities:

1) The TOE supports the association of user levels with user IDs and the association of command access levels with commands. Only one access level number can be associated with a command at a time and only one user level can be associated with a user, so the assignment is unambiguous.
2) The system users are defined in 3 levels:
   - Administrator: Perform all configuration operations. Maintain and manage the device, perform security management, create other user including administrator, operator and common user accounts.
   - Operator: Perform basic configuration operations for the service and device.
   - Common User: Perform basic system operations and simple query operations.
3) The TOE mandates that a user can only execute a specific command if his user level is equal or higher to the command access level of the specific command.
4) The TOE requires the user to be successfully identified before he can perform any other TSF-mediated actions except authentication according to section 5.1 when connecting to the TOE. If the user accesses the TOE through an RMT, the user must establish a secure remote session to the TOE prior to user authentication. The username is used for identification and the user level of the user is used for access control.
5) The TOE has a default user account named “root”, and the user level of “root” is administrator. The TOE allows only users with sufficient user level to specify alternative default values or initial values for command access levels and user levels.

(FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.3/ACFATD, FMT_SMR.1)

# 6.3 Auditing

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

1) The TOE supports generation of audit records for the following events:
   - User login and logout
   - Adding, deleting or modifying a user account
   - Password change by the user
   - Changing of command and user level
   - Session termination
   - Modification of authentication policy
   - Configuration of the device (i.e. operation requests)

- Modification of logging policy

2) The TOE records within each audit record the date and time, operation object (if applicable), access IP address (if applicable), date and time, the outcome, and user name (if applicable).

3) The TOE supports association of audit events resulting from actions of identified users with the identity of the user that caused the event.

4) The TOE allows all authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for reading audit records) to read the audit records.

5) The TOE writes audit event information to the NVRAM first (buffer). The TOE supports local storage of audit event information in the internal NOR flash memory, and output of audit event information to external audit servers.

6) The size of the log file (the file name is log.log) is configurable by the administrator with value 4M/8M/16M/32M bytes. The default maximum size of each information file is 8 MB. When the size of log.log exceeds the configured maximum size, the log.log is compressed into a smaller file in standard log_slot ID_time.log.zip format. The storage space for log.log and compressed log file in flash is about 14M, and when the storage space occupancy exceeds 70%, the system deletes oldest compressed files to save the latest compressed log file. The unauthorized users are disallowed to handle the audit records.

7) The TOE supports to report audit records to specified external SYSLOG servers.

8) The TOE does not support modification and deletion of single audit events.

9) If the audit trail in the NVRAM buffer exceeds 100kB, the TOE automatically forwards the audit data to the permanent storage location (either NOR flash or USB mass storage devices) and clears the NVRAM buffer afterwards.

10) Audit functionality is activated by default and cannot be deactivated.

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

# 6.4 Communication Security

The TOE provides communication security by the following mechanisms:

1) The TOE provides mechanisms to establish a trusted path between itself and a RMT based on the SSH2.0 protocol (SSH is sometimes also referred to STELNET).

2) The TOE permits remote users to initiate communication with the TOE to establish the trusted path.

3) The TOE supports mechanisms to verify the validity of the authentication information of SSH and can generate evidence about that which can be verified by SSH. For client authentication the TOE supports publickey authentication according to chap. 7 [RFC 4252]. Server authentication is performed using RSA according to chap. 3 [RFC 8332], rsa-sha2-256 and rsa-sha2-512.

4) The TOE denies the establishment of a trusted path in case of authentication failures or if the source IP address is prohibited to establish a trusted path according to ACL definitions.

5) The TOE supports termination of an interactive SSH session after a given interval of user inactivity. This results in a loss of user authentication (for both, connections via console as well as via RMT).

6) The TOE makes temporary session keys stored in volatile memory inaccessible upon termination of

SSH sessions.

(FTA_SSL.3, FTA_TSE.1, FTP_TRP.1/SSH)

# 6.5 Management Traffic Flow Control

The TOE supports Access Control Lists (ACLs) to deny unwanted network traffic between network elements in the management network and the TOE.

1) The TOE supports ACLs by associating ACLs to whitelists and blacklists. This function is achieved by interpreting ACL configurations then storing interpreted values in memory.
2) The TOE supports ACLs, which are based on the upper-layer protocol number, the source and destination IP addresses, the source and destination port numbers, and the packet direction.
3) The TOE permits an information flow between controlled subjects if all information security attributes are permitted by ACL. Packets not matching the ACL are logged and discarded by the router.
4) The TOE restricts the ability to read, modify and delete entries in ACLs to users with sufficient access rights.

(FDP_IFC.1, FDP_IFF.1, FMT_MSA.1/IFF, FMT_MSA.3/IFF, FMT_SMF.1)

# 6.6 Security Management

The TOE offers management functionality for its security functions. Security management functionality can either be used through LMT or RMT. For RMT, SSHv2 must be used.

The access control mechanisms of the TOE are based on hierarchical access levels where a user level is associated with every user on the one hand and a command level is associated with every command. Only if the user level is equal or higher to a specific command, the user is authorized to execute this command. Management of security function is realized through commands. So for every management function sufficient user level is required for the user to be able to execute the corresponding command.

Modifications have to be saved; otherwise they will be lost after reboot of the TOE. The TOE loads the saved device configuration during start-up, so saved modifications are not lost by rebooting the device. After reset to factory defaults, the TOE is in the factory configuration.

The security management functionality comprises:

1) The TOE support configuration of ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
2) Support configuration on limiting access for remote administration by IP address;
3) The TOE supports the configuration of the minimum time a user account is blocked after failed attempts for user authentication;
4) The TOE supports the management of user accounts (creating, maintaining, and deleting user accounts) and user data (username, password including password reset). The TOE supports the assignment of user levels to users;

5) The TOE supports the assignment and maintenance of command access levels to commands and by this defining and maintaining command groups;

6) The TOE supports the configuration of the output host and output channel for audit data (e.g. output to external audit servers);

7) The TOE supports enabling and disabling SSH for the communication between RMT and the TOE.

8) The TOE supports the configuration of the authentication policy including local authentication and remote authentication via RADIUS.

9) The TOE supports the configuration of local time and time synchronization policy via NTP.

(FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD, FMT_MSA.3/IFF, FMT_SMF.1, FMT_SMR.1)

# 7 Abbreviations, Terminology, and References

## 7.1 Abbreviations

| Name | Explanation |
|---|---|
| **AAA** | Authentication Authorization Accounting |
| **ACL** | Access Control List |
| **CC** | Common Criteria |
| **CLI** | Command Line Interface |
| **DH** | Diffie-Hellman |
| **EAL** | Evaluation Assurance Level |
| **FTTH** | Fiber To The Home |
| **FTTD** | Fiber To The Door |
| **FTTB** | Fiber To The Building |
| **FTTC** | Fiber To The Curb |
| **GPON** | Gigabit-capable Passive Optical Networks |
| **IP** | Internet Protocol |
| **IPC** | Inter-Process Communication |
| **LMT** | Local Maintenance Terminal |
| **NTP** | Network Time Protocal |

| Name | Explanation |
|---|---|
| **OLT** | Optical Line Terminal |
| **ONT** | Optical Network Terminal |
| **OPEX** | Operating Expense |
| **PP** | Protection Profile |
| **RMT** | Remote Maintenance Terminal |
| **SFP** | Security Function Policies |
| **SFR** | Security Functional Requirement |
| **SSH** | Secure Shell |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functions |
| **VRP** | Versatile Routing Platform |
| **VTY** | Virtual Type Terminal |

# 7.2 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.

| Terminology | Explanation |
|---|---|
| **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. Since all user levels are assigned to commands and users and users can only execute a command if their associated level is equal or higher compared to the level assigned to a command, a user might have certain administrative privileges but lacking some other administrative privileges. So the decision whether a user is also an administrator or not might change with the context (e.g. might be able to change audit settings but cannot perform user management). |
| **Operator:** | See User. |
| **User:** | A user is a human or a product/application using the TOE which is able to authenticate successfully to the TOE. A user is therefore different to a subject which is just sending traffic through the device without any authentication. |

# 7.3 References

| Name | Description |
|---|---|
| **[CC]** | Common Criteria for Information Technology Security Evaluation. Part 1-3<br>April 2017<br>Version 3.1<br>Revision 5<br>CCMB-2017-001, -002, -003 |
| **[FIPS 180-4]** | FIPS PUB 180-4 – Secure Hash Standard (SHS) |
| **[FIPS 186-4]** | FIPS PUB 186-4 – Digital Signature Standard (DSS), July 2013 |
| **[FIPS 197]** | FIPS PUB 197 – Advanced Encryption Standard (AES), November 26, 2001 |
| **[FIPS 198-1]** | FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC), July 2008 |
| **[NIST SP 800-38A]** | NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001 |
| **[NIST SP 800-38D]** | NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007 |
| **[NIST SP 800-56A]** | NIST Special Publication SP800-56A Revision 3 - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Apr 2018 |
| **[PKCS#1 V2.1]** | PKCS #1 v2.1: RSA Cryptography Standard, April 2004 |

| Name | Description |
|---|---|
| **[PKCS#3]** | PKCS #3: Diffie-Hellman Key- Agreement Standard, version 1.4, November 1993 |
| **[RFC 2104]** | RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997 |
| **[RFC 3526]** | RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003 |
| **[RFC 3447]** | Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003 |
| **[RFC 4251]** | The Secure Shell (SSH) Protocol Architecture, January 2006 |
| **[RFC 4252]** | The Secure Shell (SSH) Authentication Protocol, January 2006 |
| **[RFC 4253]** | The Secure Shell (SSH) Transport Layer Protocol, January 2006 |
| **[RFC 4254]** | The Secure Shell (SSH) Connection Protocol, January 2006 |
| [RFC4344] | The Secure Shell (SSH) Transport Layer Encryption Modes |
| **[RFC 5647]** | AES Galois Counter Mode for the Secure Shell Transport Layer Protocol |
| **[RFC 6668]** | SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol |
| **[RFC 8332]** | Use of RSA keys with SHA-256 and SHA-512 in the Secure Shell (SSH) protocol |