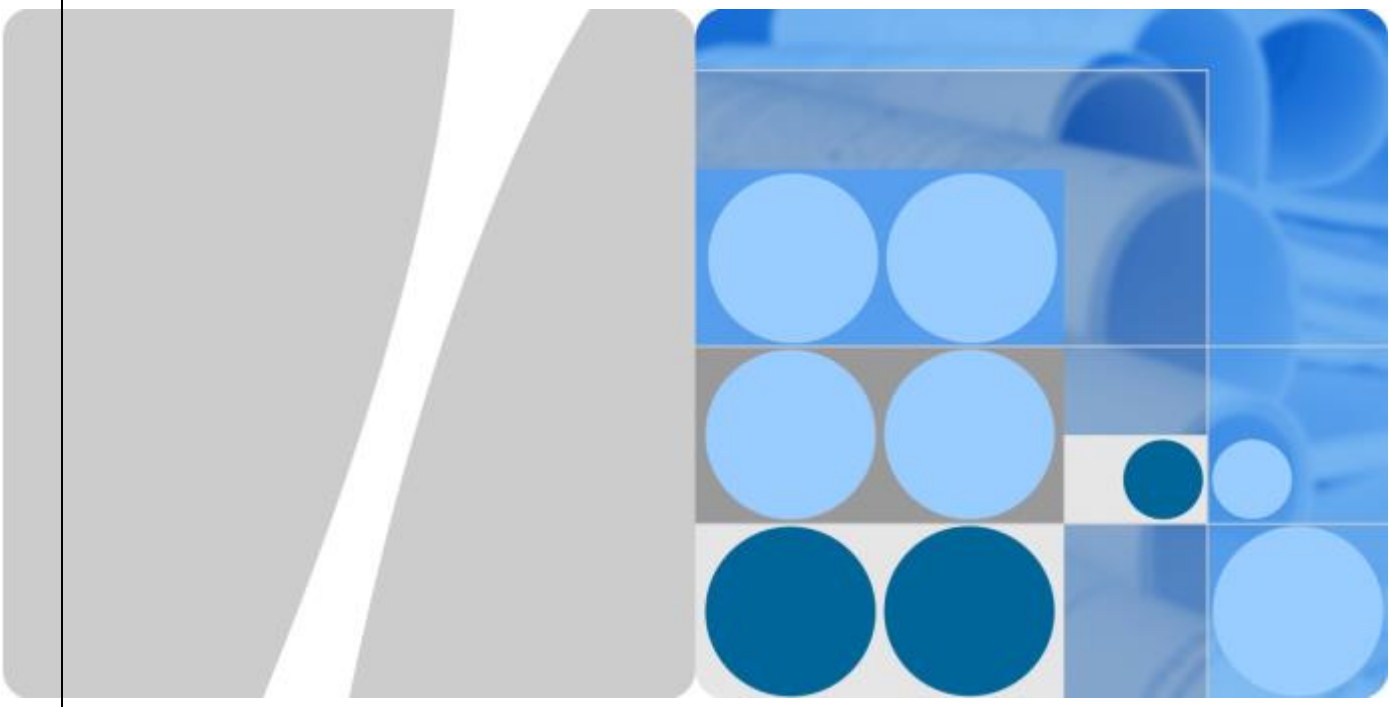


# Huawei Access Terminal Platform ATP V200R001C03

# Security Target

**Issue** V1.71

**Date** 2016-11-3

**HUAWEI TECHNOLOGIES CO., LTD.**

**Trademarks and Permissions**


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

**Notice**

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://e.huawei.com

# About This Document

## Purpose

This document provides description about ST (Security Target).

## Change History

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

| Date | Revision Version | Section Number | Change Description | Author |
|---|---|---|---|---|
| 2015-11-5 | 1.0 | ALL | Initial Draft | Shu Pingfen<br>Zhou Xuezhong<br>Huang wei<br>Sun Bo<br>Liu Wen |
| 2016-01-05 | 1.1 | 1.4.2 | Change the physical product to “B525” | Huxiaodong |
| 2016-01-13 | 1.2 | ALL | Update by review | Shupingfen |
| 2016-02-16 | 1.3 | ALL | Update by review | Shupingfen |
| 2016-03-15 | 1.4 | ALL | Update template | Shupingfen |
| 2016-06-07 | 1.5 | 1.2/1.3/1.4.1/6.3.2/6.4/6.5/8.1 | Resolve the laboratory issue | Shupingfen |
| 2016-10-21 | 1.6 | 1.4.2.5/6.3.7.2/7.1.5.1 | Modify the description about the maximum concurrent sessions | Shupingfen |
| 2016-11-2 | 1.7 | 4.3.2/6.4.1/6.4.2/7.1 | Update by review | Shupingfen |

| | | | | |
|---|---|---|---|---|
| 2016-11-3 | 1.71 | 7.1 | Update by review | Shupingfen |

# Contents

# List of Tables

# List of Figures

# 1 Introduction

This Security Target is for the evaluation of the Huawei Access Terminal Platform ATP V200R001C03; the TOE consists of Access Terminal Platform (ATP), Embedded Unified Application Platform (eUAP) and the underlying OS. The software is part of the Home Gateway and LTE Router.

## 1.1 Security Target Reference

Name: Huawei Access Terminal Platform ATP V200R001C03 Security Target

Version: 1.6

Publication Date: 2016-10-21

Author: Huawei Technologies Co., Ltd.

## 1.2 Target of Evaluation (TOE) Reference

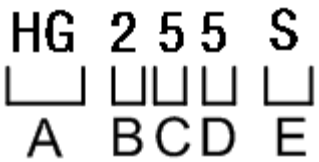
Name: Huawei Access Terminal Platform ATP V200R001C03

Version: ATP V200R001C03

Access Terminal Platform (ATP) is the software platform for home gateway, wireless router, CPE and mobile broadband products (such as Data Card, 3G/4G LTE Router and Wingle). Product software version is based on ATP software Version 2 Release 1.

Home gateway series of Huawei Access Terminal are cable broadband access products, The WAN interface is xDSL or Ethernet, and the user access interfaces including WiFi, LAN ETH port, FXS port and USB port.

The naming examples of Huawei home gateway products are as follows:

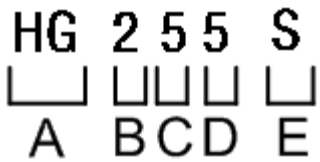



| Field | Meaning | Description |
|---|---|---|
| A | Product Series | HG: Home Gateway |

| Field | Meaning | Description |
|---|---|---|
| | | WS: Wireless Series |
| B | WAN Access technology type | • 2:Ethernet access<br>• 5:ADSL2<br>• 6: VDSL2<br>• 7:Cable |
| C | User interface service | • 2,3:WiFi<br>• 5:VOIP |
| D | | Interface changed for product upgrade |
| E(optional) | New feature for product upgrade | New feature for product upgrade, such as “S” means support USB |

Wireless router series of Huawei Access Terminal are cable broadband access products, The WAN interface is Ethernet or WiFi (As a WiFi repeater), and the user access interfaces including WiFi, LAN ETH port, and USB port.

The naming examples of Huawei wireless router products are as follows:



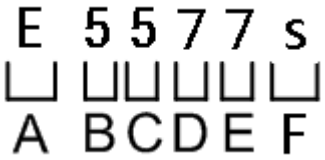

| Field | Meaning | Description |
|---|---|---|
| A | Product Series | WS: Wireless Series |
| B | WiFi Rate | • 1: 11n 150Mbps<br>• 2, 3, 4: 11n 300Mbps<br>• 5, 6: 11n 300Mbps<br>• 7, 8, 9: 11ac |
| C | Product Positioning | • 1~8: In principle, the larger the number, the higher product positioning |
| D | Product Positioning | With the second digit indicates the product positioning |
| E(optional) | Product Characteristics | Lowercase, further distinguish or identify product characteristics |

CPE products of Huawei Access Terminal are wireless broadband access products, The WAN interface is 3G/4G interface (Ethernet interface also is optional) and the user access interfaces including WiFi, LAN ETH port, FXS port and USB port.

The naming examples of Huawei CPE Access Terminal are as follows:


| Field | Meaning | Description |
|---|---|---|
| A | Product Series | B: Broadband, the uplink is 3G/4G |
| B | High/ Medium/Low end product | • 1: Low-end 3G Router<br>• 2: High end 3G Router<br>• 3: Low-end 4G LTE Router<br>• 5,6: Medium-end 4G LTE Router<br>• 7,8: High-end 4G LTE Router |
| C | Generation | • 1:First Generation<br>• 2:Second Generation |
| D | Product Serial Number | Serial number of the same grade product |
| E(optional) | Operator Code | For operator customized |

The naming examples of Huawei mobile broadband terminal products are as follows:




| Field | Meaning | Description |
|---|---|---|
| A | Product Series | • EC: CDMA+[WCDMA][WiMAX]<br>• ET: TD-SCDMA<br>• EW: WiMAX+[LTE]<br>• E: WCDMA or LTE+[ CDMA][ WCDMA]. |
| B | Product Style | • 3: Data Card<br>• 5: 3G/4G LTE Router<br>• 8: Wingle |
| C | Generation | • 1:First Generation<br>• 2:Second Generation |
| D | Communicatioin Bandwidth | • 1,2:Low speed<br>• 3:High speed |

| Field | Meaning | Description |
|---|---|---|
| | | • 5,6:Mobile WiFi<br>• 8:WiFi modem |
| E | ID Sytle | • 0,1,2,3: Direct Insert<br>• 6,7,8: Rotating plug |
| F | Chipset Vendor | • s,z:Balong<br>• u,t:Qualcomm<br>• v:infineon<br>• r: Icera<br>• y: STE |

All above product series are Access Terminal Platform products. However, The TOE is software only consisting of ATP and the underlying OS (Linux) running in the products.

Sponsor: Huawei Technologies Co., Ltd.
Developer: Huawei Technologies Co., Ltd.
Certification ID:
Keywords: Huawei, ATP, Access Terminal Platform, Access Terminals.

# 1.3 TOE Overview

ATP is a software platform for Huawei Access Terminals, which is a type of network and network-related devices and systems, support rich WAN interfaces and user access interfaces to provide WAN access, data access and voice services for home, personal and small office.

At the core of each Access Terminal is the ATP (Access Terminal Platform) deployed on SOC (System on chip) chip, the software for managing and running the gateway's access networking functionality. ATP provides extensive security features. These features include authentication control for user login; log auditing of user operation; communication and data security. SOC also supports rich type of interfaces such as Xdsl/Ethernet/3G/4G/WiFi/USB for WAN side and user side to provide internet, data, and voice access service.

The major security features of the Huawei Access Terminal products are audit, Identification & Authentication (I&A), security management, access to the product, and information flow control (i.e., network packets sent through the TOE are subject to router information flow control rules setup by the administrator or pre-defined in default configuration). The System also provides protection against the Denial of Service (DoS) attacks.

ATP is application platform based on Linux OS, so the chip platform and product hardware are non-TOE. Additionally, the operational environment is defined by the following to be outside the TOE boundary:

- A browser or APP for local administration;
- ACS for remote administration;
- HOTA servers for online upgrade;
- A Simple Network Time Protocol server for external time synchronization.

# 1.4 TOE Description

## 1.4.1 Physical scope

The following figure shows the TOE boundary, and the IT environment used for these functions in the scope of evaluation.

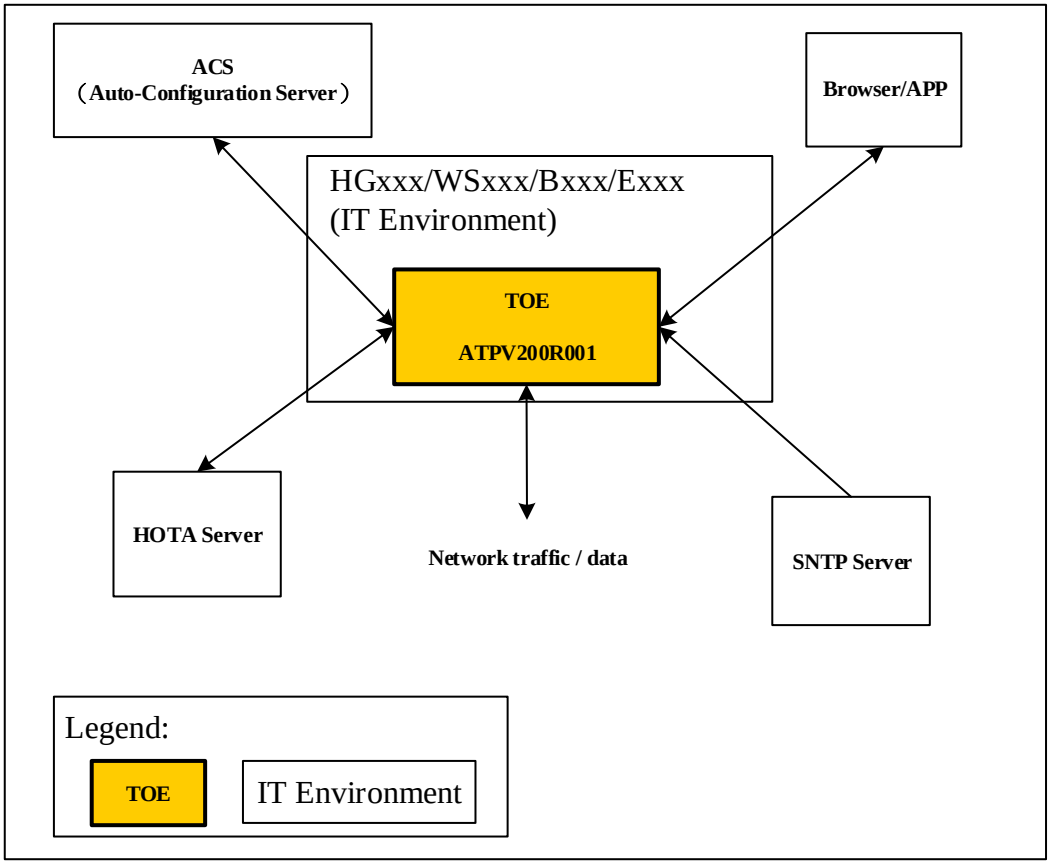



**Figure 1**: TOE Boundary

The ATP Software runs on various hardware products (HGxxx/WSxxx/Bxxx/Exxx) but the hardware platforms are excluded. ACS for limited remote administration (used by ISP), browser/APP access for local administration (Browser used by the end user and ISP and APP used only by the end user), HOTA servers for online upgrade, and a Simple Network Time Protocol (SNTP) server for external time synchronization. All TSFIs are evaluated.

The following figure shows the ATP system architecture:

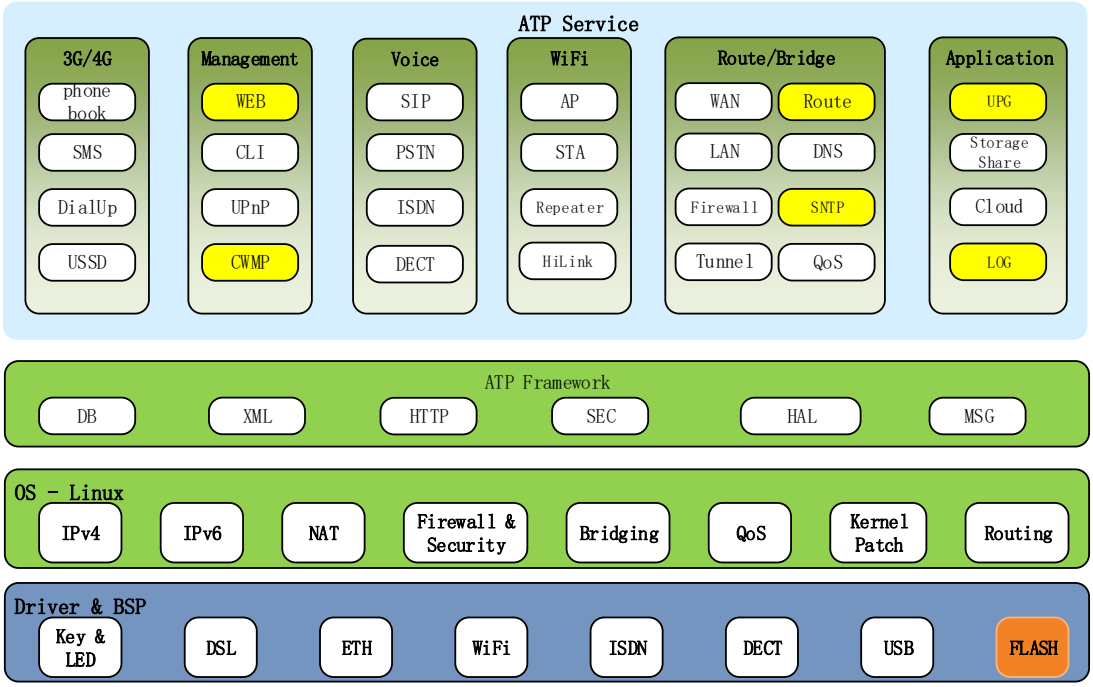



**Figure 2**: ATP System Architecture

The Subsystems with yellow background are evaluated and will be detailed in TDS. This document gives a brief description:

- WEB provides local management from Web GUI
- CWMP provides remote management by ACS according to TR-069 protocol.
- Route makes the device to forward packets from LAN to WAN
- SNTP Client is used to synchronize the network time from SNTP Server.
- UPG model is used for online upgrading.
- LOG model is used for audit and records system log.

The typical LTE router series B525 will be used to run the ATP software during this evaluation. B525 is customer premises equipment (CPE). On the network side, it provides a high-speed LTE CAT6 for wide area network (WAN) access. B525 provides internet access with highest bandwidth and speed for customers.

For users, the B525 supports both the 2.4 GHz and 5 GHz Wi-Fi functions, it provides dual concurrent 802.11b/g/n (2.4 GHz) and 802.11a/n/ac (5 GHz) interfaces, one USB interface, one phone interfaces and four Ethernet interfaces for home users to connect various terminals, such as a PC, an IP set-top box. By integrating the Foreign Exchange Station (FXS) module, the B525 can be set to voice over Internet protocol (VoIP) or circuit switch (CS) voice mode.


**Figure 3:** Interfaces on the B525

| No. | Interface | Description |
|---|---|---|
| 1 | SIM card slot | Used to insert a SIM card. |
| 2 | Phone interfaces | Used to connect the B525 to telephones. |
| 3 | USB interface | Used to connect a USB device, such as a USB flash drive. |
| 4 | LAN/WAN interfaces | Used to connect Ethernet devices, such as PCs and switches, to the B525.<br><br>One RJ45 interface support LAN/WAN function. |
| 5 | Reset button | Used to restore the factory settings of the B525. |
| 6 | Power interface | Used to connect the B525 to the power adapter. |
| 7 | On/Off button | Used to power on or off the B525. |
| 8 | WPS button | Used to enable the WPS negotiation function. |

**Table 1** Technical specifications of the B525

| Item | Description | |
|---|---|---|
| Technical standard | WAN | • Mobile Network: LTE/DC-HSPA+/HSPA+/HSPA/WCDMA/EDGE/GPRS/GSM<br>• Gigabit Ethernet: IEEE 802.3/802.3u |

| Item | Description | |
|---|---|---|
| | LAN | IEEE 802.3/802.3u |
| | WLAN | IEEE 802.11b/g/n<br>IEEE 802.11a/n/ac |
| External port | ● One power adapter port<br>● Three LAN ports (RJ45)<br>● One WAN/LAN port (RJ45)<br>● One USB 2.0 host port<br>● One phone port (RJ11)<br>● Two external LTE antenna ports (SMA-J1.5)<br>● One SIM card slot | |
| Button | ● One Power ON or OFF switch<br>● One WPS button<br>● One Reset button | |

## 1.4.2 Logical scope

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Audit
2. Identification and Authentication
3. User Data Protection
4. Security Management
5. TOE Access
6. TSF Protection
7. Trusted Path/Channels

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

### 1.4.2.1 Audit

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The TOE also generates audit records for all user activities on the management plane and stores the audit records in FLASH memory by FIFO mode in the TOE. Limit the number of stores to the FIFO (usually 100 items), save to the Flash in the way of the loop, and then cover the earliest of the low priority records.

### 1.4.2.2 Identification and Authentication (I&A)

The TOE can be managed by Web GUI. It authenticates the local user based on username and password. The TOE also provides authentication failure handling and the ability for the administrator to define password complexity requirements.

Authentication is enforced for WiFi station access if TOE acts as a WiFi AP (such as home gateway/wireless router). WiFi access authentication is not evaluated since the authentication is according to WiFi standard completely.

For home gateway and CPE, the ISP could customize the remote management by TR-069. TR-069 authentication method is according to the standard, such as HTTP basic, HTTP Digest and Certification authentication, which depends on the ACS （Automatic Configuration Server）.However, the document will not focus on this since it depends on the ISP's network environment absolutely.

#### 1.4.2.3 User Data Protection (Information flow control)

The TOE provides firewall and packet filtering as information flow control policy for the network packets sent through the TOE. The TOE provides ACL as information flow control policy for the network packets sent to the TOE (The destination IP address is the TOE).

#### 1.4.2.4 Security Management

The TOE offers management functionality for its security functions. Security management functionality can be executed by the administrator through Web UI or ACS. However, ACS remote management need to be customized by ISP, and it is not a common function.

#### 1.4.2.5 TOE Access

Mechanisms place controls on administrators' sessions. Web administrator's sessions are dropped after a pre-defined time (can be modified by ACS) period of inactivity. Dropping the connection of Web session (after the specified time period) reduces the risk of someone accessing the machines where the session was established, thus gaining unauthorized access to the session. Administrator can initiate the termination of Web sessions by clicking the "Logout" button. The TOE will deny session establishment based on maximum number of concurrent Web management sessions or maximum http connections that have been established.

#### 1.4.2.6 TSF Protection

The TOE supports importing/exporting configuration file and online upgrade. Digital sign algorithm RSA2048 (SHA256) is used to protect the data integrity for the configuration file and image file. Besides, encryption technique is used to prevent the configuration file and image file from information disclosure.

#### 1.4.2.7 Trusted Path/Channels

The TOE supports the use of a trusted path (HTTPs) for user authentication in local management and which is mandatory in remote management with Web UI. However, access from WAN side is disabled by default.

TR069 remote management supports the use of a trusted channel (HTTPs). Using HTTP or HTTPS depends on the ISP who deploys the ACS. However, the TOE supports setting the ACS server URL to use HTTPS only, and then the management traffic will be transfer through a security channel.

WiFi channel used WPA2 authentication and AES decryption is trusted. Usually, the product with WiFi AP feature uses WPA2+AES as the default configuration. A security risk notification will be prompted if unsecure authentication mode is used.

# 2 CC Conformance Claim

This ST is CC Part 1 conformant [CC], CC Part 2 conformant [CC] and CC Part 3 conformant [CC], no extended. 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 EAL2 without augmentations.

# 3 TOE Security Problem Definition

## 3.1 TOE Assets

The following table includes the assets that have been considered for the TOE:

| Asset | Description |
|---|---|
| A1.Software(Image file) | The integrity and confidentiality of the system software should be protected from modification and disclosure when transmission in the management network. |
| A2. Configuration data | Configuration data includes the security related parameters under the control of the TOE (such as username and passwords used by Web login authentication), service configuration, and audit records. The integrity and confidentiality of the configuration data should be protected. |
| A3.Network traffic | The TOE provides the Internet service (or IPTV service) and VoIP service for the end user. The network traffic includes the user data packets transferred in the air interface (LTE) or ETH/DSL interface. |

## 3.2 Threats Agent

This section shows the threats agent to the TOE. The threat agents can be categorized as the following:

| Agent | Description |
|---|---|
| Internet attacker | An attacker in the Internet is able to capture the data packets, intercept and tamper with the data that sent or received by the TOE. Information disclosure will happen if the attacker capture or intercept the packets since data transmission based on an unsecure channel. The Internet attacker can also send a large number of packets or invalid packets to cause the device denial of service. |
| LAN attacker | An attacker in the LAN side is able to spoofing valid user once the WiFi password was cracked or unsecure WiFi authentication mode was used. The attacker can rub network or even modify the device |

| | |
|---|---|
| | configuration. |

# 3.3 Threats

The assumed security threats are listed below.

| **Threat: T. UnauthenticatedAccess** | |
|---|---|
| Attack | A subject that is not an authenticated user of the TOE gains access to the TOE and modifies TOE configuration data without permission. |
| Asset | A2.Configuration data |
| Agent | Internet attacker & LAN attacker |

| **Threat: T.UnattendedSession** | |
|---|---|
| Attack | A user may gain unauthorized access to an unattended session and view and change the TOE configuration. |
| Asset | A2.Configuration data |
| Agent | Internet attacker & LAN attacker |

| **Threat: T.UpdateCompromise** | |
|---|---|
| Attack | Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration. |
| Asset | A1.Software(Image file) |
| Agent | Internet attacker & LAN attacker |

| **Threat: T.UnwantedNetworkTraffic** | |
|---|---|
| Attack | Unwanted network traffic sent to the TOE from Internet will cause the TOE's processing capacity for incoming network traffic to be consumed |

| | |
|---|---|
| | thus failing to process legitimate traffic.<br>This may further causes the TOE fails to respond to system control and security management operations. The TOE will be able to recover from this kind of situations. |
| Asset | A3.Network traffic |
| Agent | Internet attacker |

| **Threat: T.UnsecureManagementChannels** | |
|---|---|
| Attack | Threat agents may attempt to target network devices that do not use standardized secure tunnel protocols to protect the critical network traffic. Attackers may take advantage of unsecure protocol or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the management network traffic, and potentially could lead to a compromise of the network device itself. |
| Asset | A2. Configuration data & A3.Network traffic |
| Agent | Internet attacker & LAN attacker |

## 3.4 Organizational Security Policies

NA

## 3.5 Assumptions

| **Assumption Name** | **Assumption Definition** |
|---|---|
| A.PhysicalProtection | It is assumed that the TOE is protected against unauthorized physical access. For home gateway and CPE, the direct connection by ETH port is secure. |
| A.TrustworthyUsers | It is assumed that authorized end users who own the device are trustworthy and the ISP authorized remote administrators are trustworthy. |
| A.NetworkIsolation | It is assumed that the TR069 remote management network access to the TOE is separated from the Internet service networks. |

| | |
|---|---|
| A.Support | The operational environment (STNP Server in the Internet) must provide the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records. |

# 4 Security Objectives

## 4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Authentication** The TOE must authenticate users of its user access and control the session establishment.
- **O.TOE_Access** The TOE shall provide mechanisms that control an administrator's logical access to the TOE and to explicitly deny access to specific administrators when appropriate.
- **O.TrafficControl** The TOE shall control the forwarding network traffic (i.e., individual packets) from LAN to WAN or from WAN to LAN, and drop unwanted network traffic. The TOE shall also control the network traffic to itself and forbid to access the TOE self-services from LAN or WAN side.
- **O.SoftwareIntegrity** The TOE must provide functionality to verify the integrity of the received software image file and configuration file.
- **O.Audit** The TOE shall provide functionality to generate, store and review audit records for all user activities on the management plane.
- **O.SecurityManagement** The TOE shall provide functionality to securely manage security functions provided by the TOE.
- **O.SecureManagementChannels** The TOE shall provide secure management channels to prevent the local and remote management from attack.

## 4.2 Security Objectives for the Operational Environment

- **OE. PhysicalProtection** The TOE (i.e., the complete system including attached peripherals, such as a console, USB storage device) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide segregation by deploying the management interface in TOE into a local sub-network, compared to the network interfaces in TOE serving the application (or public) network. Besides, the TOE environment shall assure that the network interfaces that allow access to the TOE's remote management interfaces are in a management network that is separated from the networks that the TOE serves over the Internet service interfaces.
- **OE.TrustworthyUsers** Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

- **OE.Support** Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

# 4.3 Security Objectives Rationale

## 4.3.1 Coverage

The following tables provide a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat and that each threat is countered by at least one objective or assumption.

| Objective | Threat |
|---|---|
| O.Authentication | T.UnauthenticatedAccess |
| O.TOE_Access | T.UnattendedSession |
| O.TrafficControl | T.UnwantedNetworkTraffic |
| O.SoftwareIntegrity | T.UpdateCompromise |
| O.Audit | T.UnauthenticatedAccess<br>T.UnattendedSession |
| O.SecurityManagement | T.UnauthenticatedAccess |
| O.SecureManagementChannels | T.UnsecureManagementChannels |

**Table 2** Mapping of security objectives

## 4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

| Threat | Rationale for security objectives |
|---|---|
| T.UnauthenticatedAccess | The threat T1.UnauthenticatedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism.<br>The security objective for the operational environment OE.TrustworthyUsers contributes to the mitigation of this threat requiring the users to be responsible with their passwords.<br>The security objective for the operational environment |

| | |
|---|---|
| | OE.PhysicalProtection contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE will not be modified.<br>In addition, actions are logged allowing detection of attempts and possibly tracing of attacker (O.Audit). And Authentication mechanisms can be configured by users with sufficient user level (O.SecurityManagement). |
| T.UnattendedSession | The O.TOE_ACCESS objective requires that the TOE mitigate this threat by including mechanisms that place controls on administrator's sessions. Web sessions are dropped after a pre-defined time period of inactivity. Dropping the connection of a Web session (after the specified time period) reduces the risk of someone accessing the local and remote machines where the session was established, thus gaining unauthorized access to the session. |
| T.UpdateCompromise | This threat is countered by O.SoftwareIntegrity: when a software package is loaded, its signature is verified. |
| T.UnwantedNetworkTraffic | The threat T.nwantedNetworkTraffic is directly counteracted by the security objective for the TOE O.TrafficControl. ACL and packet filter can also deny unwanted network traffic enter or passthrough TOE. |
| T.UnsecureManagementChannels | The threat T. UnsecureManagementChannels is countered by O.SecureManagementChannels which establishes a secure communication channel between the TOE and external entities in the management network. |

**Table 3** *Sufficiency analysis for threats*

The following rationale provides justification that the security objective and assumption for the environment is one-one correspondence, when security objectives achieved, actually contributes to the environment achieving consistency with the assumption.

| **Assumption** | **Rationale for security objectives** |
|---|---|
| A.PhysicalProtection | This assumption is directly implemented by the security objective for the environment OE.PhysicalProtection. |
| A.TrustworthyUsers | This assumption is directly implemented by the security objective for the environment OE.TrustworthyUsers. |
| A.NetworkSegregation | This assumption is directly implemented by the security objective for the environment OE.NetworkSegregation. |
| A.Support | This assumption is directly implemented by the security |

| | |
|---|---|
| | objective for the environment OE.Support. |

**Table 4** *Sufficiency analysis for assumption*

# 5 Extended Components Definition

No extended components have been defined for this ST.

# 6 Security Requirements

This section provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

## 6.1 Conventions

The following conventions are used for indicating different content:

- **Bold text** indicates the content is the same with CC part2 document.
- ***Italicized and bold text*** indicates the completion of an assignment or a selection.
- (Underlined text in parentheses) indicates additional text provided as a refinement.
- Iteration/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

## 6.2 Definition of security policies

To avoid redundancy in the definition of SFRs, in this chapter the security policies are defined that have to be fulfilled by the TOE.

### 6.2.1 ATP information control policy

The ATP information control policy defines the following subjects and attributes:

Subjects:

- network packets

Information security attributes:

- source IP address,
- destination IP address,
- transport protocol,

- source TCP or UDP port number,
- destination TCP or UDP port number,
- source MAC address (used in parent control and WLAN MAC filtering),

Whenever an incoming network packet is intended to be forwarded, the ATP information control policy mandates to check the Access Control List (ACL) defined for ATP. The rules in ACL refer to handling of the network packet on layer 3.

Whenever an outcoming network packet is intended to be forwarded, Rules for layer 2 could either permit or deny forwarding based on the information security attributes 'source MAC address'. The network packet is dropped or forwarded depends on the rule matches with whitelist or blacklist rule.

Rules for layer 3 could either permit or deny forwarding based on the information security attributes 'source IP address', 'destination IP address', 'transport protocol', 'source TCP or UDP port number', 'destination TCP or UDP port number'. Rules have to contain at least one of the attributes but may contain several attributes.

For every incoming network packet that is intended to be forwarded the ACL is checked for a rule that matches the attributes of the packet or frame, respectively starting from the first entry in the ACL. The ACL is checked until the first matching rule is found. The network packet is then either forwarded or discarded according to the matching rule in the ACL. If no matching rule is found, the network packet is discarded.

# 6.3 TOE Security Functional Requirements

## 6.3.1 Security Audit (FAU)

### 6.3.1.1 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 [selection: *not specified*] level of audit; and**
**c) [assignment: *The following auditable events:***

**All user activities on the management plane are recorded in system logs, including:**

***1) Login and logout***

***2) Changing user account: username, password***

***3) Locking, unlocking user account***

***4) Changing system security configurations***

***5) Import/Export configuration file***

***6) Modifying configuration parameters***

***7) Reboot, restore default settings***

***8) Upgrading software remotely or locally*]**

Application Note: Audit functionality shall be enabled by default. Disabling audit functionality is impossible by Web GUI.

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

a) **Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and**
b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *User ID (if applicable), configure tool (if applicable), workstation IP (if applicable)*].**

Application Note: The term 'if applicable' shall be read as 'whenever an event can be associated with the specified information'. For example if an event can be associated with a User ID, then the event shall be audited and the audit information shall contain the User ID. If the event cannot be associated with the User ID, the event shall be audited and the audit information shall not contain User ID information. If multiple conditional information can be associated with an event (e.g. User ID and configure tool can be associated with an event), all the conditional information shall be contained in the audit information when auditing the event.

### 6.3.1.2 FAU_GEN.2 User identity association

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

### 6.3.1.3 FAU_SAR.1 Audit review

**FAU_SAR.1.1 The TSF shall provide [assignment: *users with audit review rights*] with the capability to read [assignment: *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.**

Application note: This SFR can be observed through Web GUI.

### 6.3.1.4 FAU_SAR.3 Selectable Audit review

**FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: *selection*] of audit data based on [assignment: *log level (0 Emergency;1 Alert;2 Critical;3 Error;4 Warning;5 Notice;6 Informational) and log type (ALL, User Level, System, Security)*].**

Application note: This SFR can be observed through Web GUI.

### 6.3.1.5 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 [selection: *prevent*] unauthorized modifications to the stored audit records in the audit trail.**

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

**FAU_STG.3.1 The TSF shall [assignment: *overwritten the oldest records*] if the audit trail exceeds [assignment: *the pre-defined limited 100 records*].**

Application Note: There are several options to store audit data. At first they are written to RAM and from there they can be written to Flash, or external audit servers (if present). When the audit trail in RAM exceeds 100 records the oldest audit data is overwritten.

### 6.3.2 Cryptographic Support (FCS)

#### 6.3.2.1 FCS_COP.1(1)/AES Cryptographic operation

**FCS_COP.1.1 The TSF shall perform [assignment: *symmetric decryption and encryption*] in accordance with a specified cryptographic algorithm [assignment: *AES256 or AES128*] and cryptographic key size [assignment: *256 or 128 bits*] that meet the following: [assignment: *[FIPS 197]*].**

#### 6.3.2.2 FCS_COP.1(2)/RSA Cryptographic operation

**FCS_COP.1.1 The TSF shall perform [assignment: *asymmetric authentication*] in accordance with a specified cryptographic algorithm [assignment: *RSA*] and cryptographic key sizes [assignment: *2048 bits*] that meet the following: [assignment: *[FIPS 186-2], RSA Cryptography Standard ([PKCS#1 V1.5])*].**

#### 6.3.2.3 FCS_COP.1(3)/SHA256 Cryptographic operation

**FCS_COP.1.1 The TSF shall perform [assignment: *data integrity verification*] in accordance with a specified cryptographic algorithm [assignment: *SHA256*] that meet the following: [assignment: *[FIPS 198]*].**

#### 6.3.2.4 FCS_CKM.1(1)/AES Cryptographic key generation

**FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *PRNG*] and specified cryptographic key sizes [assignment: *128 or 256 bits*] that meet the following: [assignment: *[RFC 1750]*].**

#### 6.3.2.5 FCS_CKM.1(2)/RSA Cryptographic key generation

**FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *keygen method RSA*] and specified cryptographic key sizes [assignment: *2048 bits*] that meet the following: [assignment: *RSA Cryptography Standard [PKCS#1V1.5]*].**

#### 6.3.2.6 FCS_CKM.4(1)/AES Cryptographic key destruction

**FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *AES cryptographic key used for sensitive data storage encryption is destructed periodically (160 days)]* that meets the following: [assignment: *[RFC 1750]*]].**

#### 6.3.2.7 FCS_CKM.4(2)/RSA Cryptographic key destruction

**FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *RSA cryptographic key used for Web sensitive data transmission encryption is destructed when the device is reboot*] that meets the following: [assignment: *RSA Cryptography Standard [PKCS#1V1.5]*].**

## 6.3.3 User Data Protection (FDP)

### 6.3.3.1 FDP_IFC.1 Subset information flow control

**FDP_IFC.1.1 The TSF shall enforce the [assignment: *ATP information control policy as defined in chap.* 6.2.1] on [assignment: *the network traffic, the ACL-defined information, and rules defined in the rules either permitting or denying forwarding of the network traffic based on Information Security attributes as defined in chap.* 6.2.1].**

### 6.3.3.2 FDP_IFF.1 Simple security attributes

**FDP_IFF.1.1 The TSF shall enforce the [assignment: *ATP information control policy as defined in chap.* 6.2.1] based on the following types of subject and information security attributes:**

**[assignment:**

***Subjects:***

- ***network packets or frames,***

***Information security attributes:***

- ***source IP address,***
- ***destination IP address,***
- ***transport protocol,***
- ***source TCP or UDP port number,***
- ***destination TCP or UDP port number,***
- ***source MAC address*]**

**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: [assignment: *the ATP information control policy as defined in chap.* 6.2.1*, and the policy's action is permit.*]**

**FDP_IFF.1.3 The TSF shall enforce the [assignment: *ATP information control policy as defined in chap.*6.2.1].**

**FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *None*].**

**FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *None*].**

## 6.3.4 Identification and Authentication (FIA)

### 6.3.4.1 FIA_AFL.1 Authentication failure handling

**FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: 3]*] *unsuccessful authentication attempts* occur related to [assignment: *since the last successful authentication of the indicated user identity*].**

**FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *surpassed*], the TSF shall [assignment: *terminate the session of the user trying to authenticate and block the client IP address for authentication for 1 minute. The locking time will be doubled for the subsequent 3 consecutive failed authentication attempts, 64 minutes is the maximum time*].**

### 6.3.4.2 FIA_ATD.1 User attribute definition

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

- ***a)*** ***user ID***
- ***b)*** ***user level***
- ***c)*** ***SHA256 hash of password***
- ***d)*** ***temporary blocking time for user accounts after unsuccessful authentication attempts***
- **e)** ***time when user is logging in and logging off*]**

### 6.3.4.3 FIA_SOS.1 Verification of secrets

**FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *for web user, the password must meet the following:***

***1) a minimum length (characters): default 6 and within a range of 6-32;***

***2) Complexity requirements: must contain at least two of the following character types:***

- ***a)*** ***At least one (1) numeric character must be present in the password;***
- ***b)*** ***At least one (1) special character must be present in the password. Special characters include: ~!@#$%^&*()_+|{}:"<>?`-=\[];';***
- ***c)*** ***At least one (1) upper case character; and***
- ***d)*** ***At least one (1) lower case character;].***

### 6.3.4.4 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.**

Application Note: Authentication is possible by username and password.

### 6.3.4.5 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.**

Application Note: Authentication is possible by username and password. The user is identified by his username if he is able to successfully authenticate with his username and corresponding password.

#### 6.3.4.6 FIA_UAU.6 Re-authenticating

**FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment:**

- ***a) user changes password***
- ***b) session timeout***
- **c) *logout*]**

#### 6.3.4.7 FIA_UAU.7 Protected authentication feedback

**FIA_UAU.7.1 The TSF shall provide only [assignment: *obscured feedback*] to the user while the authentication is in progress.**

### 6.3.5 Security Management (FMT)

#### 6.3.5.1 FMT_MOF.1 Management of security functions behaviour

**FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behavior of*] the functions [assignment: *listed in the following table*] to [assignment: *the administrator*].**

| Security Functions |
|---|
| Configuring Firewall |
| Configuring IP Filters |
| Configuring MAC Filters |
| Configuring Application Filters |
| Configuring ACL |
| Configuring Web Management Password |
| Configuring remote ACS administration (if applicable) |
| Configuring Login control |
| Configuring SNTP |
| Configuring Reboot |
| Configuring Restore Default Settings |

| Configuring WiFi Access Parameters |
|---|

### 6.3.5.2 FMT_MSA.1 Management of security attributes

**FMT_MSA.1.1 The TSF shall enforce the [assignment: *ATP information control policy*] to restrict the ability to [selection*: query, modify, delete*] the security attributes [assignment: *identified in FDP_IFF.1*] to [assignment: *the administrator*].**

### 6.3.5.3 FMT_MSA.3 Static attribute initialisation

**FMT_MSA.3.1 The TSF shall enforce the [assignment: *ATP information control policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.**

**FMT_MSA.3.2 The TSF shall allow [assignment: *the administrator*] to specify alternative initial values to override the default values when an object or information is created.**

### 6.3.5.4 FMT_SMF.1 Specification of Management Functions

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

- ***a) Define and maintain IP addresses and address ranges (via ACL policy) that will be accepted as source addresses for traffic forwarding (L3 forwarding). Define and maintain IP addresses and address ranges (via ACL policy) that will be accepted for local and remote administration (TOE administration).***
- ***b) Configure the firewall level.***
- ***c) Configure URL filtering, application filtering and parent control (source MAC address filtering based on time rule).***
- ***d) Manage user accounts and user data.***
- ***e) Configure audit functionality, such as configure log display level and log type***
- ***f) Perform reboot.***
- ***g) Perform restore default settings.***
- ***h) Enable or Disable SNTP function and configure SNTP Server address, time zone.***
- ***i) Configure WiFi parameters, such as WiFi SSID, key, authentication mode and encryption mode and so on.***

**]**

#### 6.3.5.5 FMT_SMR.1 Security roles

**FMT_SMR.1.1 The TSF shall maintain the roles [assignment: administrators].**

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

## 6.3.6 Protection of the TSF (FPT)

### 6.3.6.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

**FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.**

#### 6.3.6.2 FPT_ITI.1 Inter-TSF detection of modification

**FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [assignment: *digital signature*].**

**FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: *reject the update of the configuration file and image file*] if modifications are detected.**

#### 6.3.6.3 FPT_STM.1 Reliable time stamps

**FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.**

Application Note: The reliable time stamps are based on an external time source using SNTP protocol. Once the TOE synchronizes the clock with the SNTP server, the clock will be set as local time and maintains by the OS.

### 6.3.7 TOE access (FTA)

#### 6.3.7.1 FTA_SSL.3 TSF-initiated termination

**FTA_SSL.3.1 The TSF shall terminate an interactive session after [assignment: *5 minutes*].**

Application Note: The web server will terminate the current session if there is no any interaction for 5 minutes. However, the time interval of user inactivity cannot be configured by the end user.

#### 6.3.7.2 FTA_MCS.1 Basic limitation on multiple concurrent sessions

**FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.**

**FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: *128*] sessions per user.**

#### 6.3.7.3 FTA_TSE.1 TOE session establishment

**FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment:**

- ***a) authentication failure***
- ***b) ACL***
- **c) *Session connection reaches max number*].**

### 6.3.8 Trusted Path/Channels (FTP)

#### 6.3.8.1 FTP_ITC.1 Inter-TSF trusted channel

**FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.**

**FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.**

**FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *HTTPs over TR069*].**

#### 6.3.8.2 FTP_TRP.1 Trusted path

**FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *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 [selection: *modification, disclosure*].**

**FTP_TRP.1.2 The TSF shall permit [selection: *remote users*] to initiate communication via the trusted path.**

**FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*].**

Application Note: TOE supports HTTP and HTTPs when access Web GUI from LAN side. However, it depends on the end user which protocol to use. It is trustworthy when connect to the TOE by RJ45 port or WiFi with WPA2 authentication. HTTPs will be used (redirect automatically) when access Web GUI from WAN side. However, access Web GUI from WAN side is forbidden by default.

## 6.4 Security Functional Requirements Rationale

### 6.4.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

| Security Functional Requirements | Objectives |
|---|---|
| FAU_GEN.1 | O.Audit |
| FAU_GEN.2 | |
| FAU_SAR.1 | |
| FAU_SAR.3 | |
| FAU_STG.1 | |
| FAU_STG.3 | |
| FCS_COP.1(1)/AES,<br>FCS_CKM.1(1)/AES, | O.SoftwareIntegrity |

| | |
|---|---|
| FCS_CKM.4(1)/AES | |
| FCS_COP.1(2)/RSA,<br>FCS_CKM.1(2)/RSA,<br>FCS_CKM.4(2)/RSA | O.SoftwareIntegrity |
| FCS_COP.1(3)/SHA256 | O.Authentication<br>O.SoftwareIntegrity |
| FDP_IFC.1 | O.TrafficControl |
| FDP_IFF.1 | |
| FIA_AFL.1 | O.Authentication |
| FIA_ATD.1 | |
| FIA_SOS.1 | |
| FIA_UAU.2 | |
| FIA_UID.2 | |
| FIA_UAU.6 | |
| FIA_UAU.7 | |
| FMT_MOF.1 | O.SecurityManagement |
| FMT_MSA.1 | |
| FMT_MSA.3 | |
| FMT_SMF.1 | |
| FMT_SMR.1 | |
| FPT_ITC.1 | O.SoftwareIntegrity |
| FPT_ITI.1 | |
| FPT_STM.1 | O.Audit |
| FTA_SSL.3 | O.TOE_Access |

| | |
|---|---|
| FTA_MCS.1 | |
| FTA_TSE.1 | |
| FTP_ITC.1 | O.SecureManagementChannels |
| FTP_TRP.1 | |

**Table 5:** *Mapping SFRs to objectives*

## 6.4.2 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:

| **Security objectives** | **Rationale** |
|---|---|
| O.Authentication | User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. 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. Initial |
| O.TrafficControl | TOE information flow control policy is based on firewall and packet filtering as defined in FDP_IFC.1 and FDP_IFF.1 to protect the TOE from information flow attack. |
| O.TOE_Access | TOE access is implemented by FTA_MCS.1, FTA_SSL.3 and FTA_TSE.1 |
| O.SoftwareIntegrity | When a software package is loaded, its signature is verified via FCS_COP.1(3)/SHA256 and FCS_COP.1(2)/RSA. |

| | |
|---|---|
| O.SecurityManagement | The TOE is required to provide the ability to restrict the use of TOE management/administration/security functions to authorized administrators of the TOE [FMT_MOF.1]. The TOE will capable of performing security management functions. The TOE is capable of performing numerous management functions including start-up, shutdown, and creating/modifying/deleting configuration items [FMT_SMF.1].<br><br>The TOE must be able to recognize the administrative role that exists for the TOE [FMT_SMR.1].<br><br>The TOE must restrict the ability to manage security attributes associated with the UNAUTHENTICATED<br><br>SFP to the administrator. [FMT_MSA.1]<br><br>The TOE must allow the privileged administrator to specify alternate initial values when an object is created.[FMT_MSA.3].<br><br>The TOE ensures that all administrator actions resulting in the access to TOE security functions and configuration data are controlled. [FMT_SMF.1, FMT_MOF.1]<br><br>The TOE ensures that access to TOE security functions and configuration data is based on the assigned administrator role. [FMT_SMR.1] |
| O.SecureManagementChannels | The TOE is required to provide the secure management channels when management the device from local Web UI or remote ACS. [FTP_ITC.1, FTP_TRP.1]. |
| O.Audit | The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by FPT_STM.1 and user identities as defined in FAU_GEN.2 where applicable.<br><br>Requirements on reading audit records are defined in FAU_SAR.1. The protection of the stored audit records is implemented in FAU_STG.1. Functionality to overwrite the oldest audit records is provided if it exceeds 100 records is required according to FAU_STG.3. |

**Table 6:** *SFR sufficiency analysis*

### 6.4.3 Security Requirements Dependency Rationale

Dependencies within the EAL2 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

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

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

| Security Functional Requirement | Dependencies | Resolution |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 |
| FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.1 | FAU_GEN.1<br>FIA_UID.2/RTM |
| FAU_SAR.1 | FAU_GEN.1 | FAU_GEN.1 |
| FAU_STG.1 | FAU_GEN.1 | FAU_GEN.1 |
| FAU_STG.3 | FAU_STG.1 | FAU_STG.1 |
| FCS_COP.1(1)/AES | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1(1)/AES,<br>FCS_CKM.4(1)/AES |
| FCS_COP.1(2)/RSA | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1(2)/RSA<br>FCS_CKM.4(2)/RSA |
| FCS_COP.1(3)/SHA256 | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]<br>FCS_CKM.4 | N/A |
| FCS_CKM.1(1)/AES | [FCS_CKM.2 or FCS_COP.1],<br>FCS_CKM.4 | FCS_COP.1(1)/AES,<br>FCS_CKM.4(1)/AES |
| FCS_CKM.1(2)/RSA | [FCS_CKM.2 or FCS_COP.1],<br>FCS_CKM.4 | FCS_COP.1(2)/RSA ,<br>FCS_CKM.4(2)/RSA |
| FCS_CKM.4(1)/AES | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1] |

| | | |
|---|---|---|
| FCS_CKM.4(2)/RSA | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1] |
| 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 |
| FDP_DAU.1 | None | N/A |
| FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.2 |
| FIA_ATD.1 | None | N/A |
| FIA_UAU.2 | FIA_UID.1 | FIA_UID.2 |
| FIA_UID.2 | None | N/A |
| FIA_UAU.6 | None | N/A |
| FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.2 |
| FMT_MOF.1 | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_ACC.1<br>FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1<br>FMT_SMR.1 |
| FMT_SMF.1 | None | N/A |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.2 |

| | | |
|---|---|---|
| FPT_ITC.1 | None | N/A |
| FPT_ITI.1 | None | N/A |
| FPT_STM.1 | None | N/A |
| FTA_SSL.3 | None | N/A |
| FTA_MCS.1 | FIA_UID.1 | FIA_UID.2 |
| FTA_TSE.1 | None | N/A |
| FTP_TRP.1 | None | N/A |
| FTP_ITC.1 | None | N/A |

**Table 7:** *Dependencies between TOE Security Functional Requirements*

### 6.4.4 Justification for unsupported dependencies

The following dependencies are unsupported for the reasons given below.

FCS_COP.1(3)/SHA256: The dependency on FCS_CKM.1 (Key generation) and FCS_CKM.4 (Key destruction) is unsupported, because the SHA256 doesn't need to generate or destroy keys.

## 6.5 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components. No operations are applied to the assurance components.

| Assurance Class | Assurance components |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.2 Security-enforcing functional specification |
| | ADV_TDS.1 Basic design |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.2 Use of a CM system |

| | |
|---|---|
| | ALC_CMS.2 Parts of the TOE CM coverage |
| | ALC_DEL.1 Delivery procedures |
| 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.1 Evidence of coverage |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing – sample |
| AVA: Vulnerability assessment | AVA_VAN.2 Vulnerability analysis |

## 6.6 Security Assurance Requirements Rationale

The Evaluation Assurance Level 2 has been chosen to commensurate with the threat environment that is experienced by typical consumers of the TOE.

# 7 TOE Summary Specification

## 7.1 TOE Security Functional Specification

### 7.1.1 F.Audit

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
- Modifying a user account: username and password.
- Locking, unlocking user account.
- Changing system security configurations.
- Import/Export configuration file.
- Modifying configuration parameters by Web UI/ACS/CLI.
- Reboot the device (except for reboot by hardware).
- Resetting the device to factory settings
- Upgrading software remotely or locally.

2 The TOE records within each audit record the date and time of the event, type of event, subject identity (of applicable) and the outcome (success or failure) of the event. The TOE provides reliable time stamps for that purpose. Depending on the definition of the event records might include the interface, workstation IP, User ID or operations.

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 to read the audit records.

5 The TOE supports log file formats binary and readable text. This function is achieved by providing output format transformation. By this the TOE provides the user with audit information suitable for interpretation.

6 The TOE writes audit event information to the NVRAM first (buffer). The TOE supports local storage of audit event information in the internal NAND/NOR flash memory, and these audit information can be exported to storage in local device (such as local PC).

7 The TOE does not support modification of audit information.

8 The TOE restricts the ability to delete audit event information to authorized users. Only the administrator can delete the audit event information if the TOE supports two or more user levels. If there is only one user, then the user can delete the audit event information.

9 The TOE automatically overwrites the oldest audit data in the NVRAM (buffer) if the audit trail exceeds 100 records.

10 Audit functionality is activated by default and the end user cannot disable it. Logging of the event of disabling audit functionality is enforced by default.

### 7.1.2 F.I&A

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 FIA_AFL.1 The TOE supports authentication via password or username and password. This function is achieved by comparing user information input with pre-defined reference values stored in memory.
2 FIA_ATD.1, The TOE stores the following security attributes for individual uses:
- User ID
- User level
- SHA256 hash of password and salt
- Number of unsuccessful authentication attempts since last successful authentication
- Time when users are logging in and logging off

3 The TOE supports the use of HTTPs certification authentication in local management and which is mandatory in remote management with Web UI. However, access from WAN side is disabled by default.
4 The TOE supports the detection of 3 consecutive failed authentication attempts after the last successful user authentication and locks the account for one minute. The locking time will be doubled for the subsequent 3 consecutive failed authentication attempts, 64 minutes is the maximum time.
5 The TOE allows specifying minimum requirements on the length and complexity of passwords.
6 The TOE requires each user to be successfully authenticated before he can perform any other TSF-mediated actions.
7 If the authentication method is based on username and password, the username is used for identification. If the authentication method is based on password only, the terminal ID is used for identification and the terminal has to be regarded as ‘user’.

### 7.1.3 F.UserDataProtection

This section describes ATP information flow control for the network traffic sent to the TOE and sent through the TOE.

The TOE supports Access Control Lists (ACLs) to filter traffic destined to the TOE to prevent internal traffic overload and service interruption. The TOE also uses the ACL to identify flows and perform flow control to prevent the CPU and related services from being attacked. The content of ACLs is pre-defined and can be modify by Web UI or ACS.

ACL function is detailed by the following:

1 The TOE supports ACLs by associating ACLs to whitelists. This function is achieved by interpreting ACL configurations then storing interpreted values in memory.
2 The TOE supports access control for ICMP, FTP, HTTP, HTTPS services from WAN-side and LAN-side. Besides, Samba service from LAN-side access can be controlled by ACL
3 The TOE enables the LAN side ICMP, FTP, HTTP, Samba, HTTPS service, and all service on the WAN side access are disabled by default, the product can be customized.
4 The TOE supports 16 ACL rules at most. For each rule, the user can configure service

type, access direction, IP address range. If no IP address is specified, it means that any device can access the service provided by the TOE.

5 The ACL function realized based on Netfilter structure of the Linux kernel. The "iptables" commands are executed according to the ACL rules. For example, allowing ping the external IP address of the device from WAN side with IP address 100.100.100.100, the "iptables" command is: "iptables -I INPUT_SERVICE_ACL -i ppp256 -p icmp -s 100.100.100.100 -j ACCEPT".

The TOE supports IPv4 and IPv6 firewall, to prevent the external active packet access from the WAN interface. The TOE supports three firewall levels: "High", "Low" and "Disabled". They are defined as the following:

**High**: only allows DNS, FTP, HTTP/HTTPS protocol packets through the TOE, other packets are forbidden to pass through the TOE.

**Low**: allows all active packets from LAN side to the WAN side, other packets are blocked.

**Disabled**: disable the firewall, all the packets are able to pass through the TOE.

"Low" is the default level. If the end user disables the firewall by Web GUI, a security warning will be prompted.

The TOE supports SPI (Stateful Packet Inspection) and DDoS functions. The TOE protects the device from LAND attack, Ping of Death, ICMP flood, SYN flood, ARP attack and so on.

Packet Filtering is the primary functionality implemented by the TOE. The packet filtering filters packets based on the Physical interface, MAC address, IP address, port number, protocol type, and can be combined. The packet filtering function realized based on Netfilter structure of the Linux kernel. The "iptables" and "ebtables" commands are executed according to the filtering rules.

The TOE supports IP filtering by the 5-tuple (source IP address, source port, destination IP address, destination port, protocol), blacklist can be defined. Besides, MAC filtering and URL filtering are used in the parent control function.

### 7.1.4 F.Cryptographic_Functions

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

1 The TOE supports symmetric encryption and decryption using the AES algorithm in CBC mode according to [FIPS 197] and [FIPS SP 800-38A] using key lengths of 128 or 256 bits. AES-128 CBC is used for encryption and decryption in configuration file backup & restoring, sensitive data storage and image file packaging & upgrading. AES-256 CBC is used in encryption and decryption default configuration file.

2 The TOE supports hashing of data using SHA256 algorithm according to [FIPS 180-4]. Hashing is used for hashing passwords before encryption with AES-128-CBC before storage inside the TOE.

3 TOE supports data integrity generation and verification using the digital sign algorithm RSA (SHA256) using key lengths of 2048 bits. The data integrity protection mechanism is used for integrity protection for configuration file and image file upgrading.

4 The TOE supports key generation for the RSA algorithm according to [FIPS 186-4] using CRT. RSA keys generated have a key length of 2048bits and are intended for

usage with RSASSA-PKCS1-V1_5.

5 The TOE supports the destruction of RSA keys by overwriting them with 0.

6 The TOE support the generation of random numbers according to ANSI X9.31, Appendix A.2.4 based on AES 128bit, CBC mode. The deterministic random number generator provided by the TOE corresponds to the requirements of class DRG.2 according to [AIS20]. The random numbers are used for generation of 128bit or 256bit AES keys and 2048bit RSA keys.

(FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/SHA256, FCS_CKM.1/AES, FCS_CKM.1/3DES, FCS_CKM.1/RSA)

### 7.1.5 F.SecurityManagement

The TOE offers management functionality for its security functions. This section describes the security functions can be managed by Web UI or ACS. They are detailed by the following:

1 The TOE supports the configuration of firewall level.

2 The TOE supports the configuration of ACL rules. Configuration parameter Including LAN or WAN, the source IP address or IP address range, TOE self-services (ICMP, FTP, Samba, HTTP, HTTPS).

3 The TOE supports the configuration of application filtering. Including DNS, FTP Server, HTTP Proxy, Mail (POP3), Mail (SMTP), SAMBA, Secure Shell Server (SSH), Secure Web Server (HTTPS), Telnet Server, Web Server (HTTP). The TOE supports configure block these application block for one or more than one specified device.

4 The TOE supports the configuration of URL filtering. Match the key words of the domain name will be filtered.

5 The TOE supports the configuration of parent control, based on MAC address, supports by week, day, and time to control the LAN side of the device to access WAN network.

6 The TOE supports the configuration of IP address filtering function by 5-tuple (protocol, source address, source port, destination address, destination port) filter.

7 The TOE supports change the Web authentication password and TR069 parameters, including authentication information (ACS username, ACS password, connection request username and connection request password) and ACS URL, period inform interval.

8 The TOE supports view the audit records with log type and log level.

9 The TOE supports reboot the device, restore default settings.

10 The TOE supports configure WiFi parameters and SNTP parameters.

### 7.1.6 F.TOE_Access

#### 7.1.6.1 TOE Session Establishment

A Web session will be generated when the Web login successful. If the maximum number of concurrent sessions reaches 128 (Up to 10 concurrent sessions per IP address are allowed) or the maximum number of HTTP connections reaches 40 (The timeout for the HTTP connection is 45 seconds), the Web login will be rejected. A browser can generate four to six HTTP links at a time, depending on the browser model. For example, suppose a browser generates five HTTP connections without one timeout, then the maximum session can be established is eight.

#### 7.1.6.2 TSF-initiated Termination

The TOE has the ability to terminate stale (inactive) connections. The TOE terminates interactive session after a pre-defined period of inactivity with a default value of 5 minutes.

This idle-time parameter configures the idle timeout for Web sessions before the session is terminated by the system. This would reduce the chance for the unauthorized administrators to access the device through an unattended opened session. By default, an idle Web session times out after five (5) minutes of inactivity.

#### 7.1.6.3 User-initiated Termination

The administrators can initiate termination of their own sessions by clicking the logout button on the top right of the Web GUI. When "Logout" button is pressed, the current logged session will be destroy and the page which user is visiting will be redirected to the login page.

### 7.1.7 F.TSF_Protection

#### 7.1.7.1 Upload/Download Configuration file

The TOE has the ability to upload and download the configuration file of the device by Web GUI or ACS. Upload configuration file means backup the configuration to local PC (by Web) or remote HTTP/HTTPs/FTP Server (by ACS). By contraries, download configuration file means restore the configuration of the device using the backup one.

To protect the configuration file from disclosure and tampering in storage or transmission, digital sign and encryption technique are used to when uploading configuration file. Digital sign first and then encrypt. Verify the digital sign and decrypt when downloading configuration file.

#### 7.1.7.2 Online Upgrade

Online (OTA) upgrade is used for system software update. Huawei named this upgrade method with "HOTA" upgrade. HOTA Server will be deployed by Huawei.

The upgrade process is divided into two steps:

1) Check the new software version

The TOE supports the user manual trigger to check the new version and automatic check the new software version periodically.

2) Download and Upgrade

Download the image file and decrypt it, then verify the digital sign to ensure the software version is the correct one. If the decryption and verification are successful, then continue to upgrade. Otherwise, the upgrade is terminated.

The common sign server provided by Huawei is used when generated the image file to ensure the private key is trusted.

### 7.1.8 F.TrustedPath/Channels

#### 7.1.8.1 HTTPs over Web

The TOE supports the use of a trusted path (HTTPs) for user authentication and data transmission in Web management. HTTPs protocol is optional in local management and it depends on the end user. It is mandatory in remote management with Web UI. HTTPs will be

redirected When the user using HTTP protocol to access the Web service. However, access from WAN side is disabled by default.

#### 7.1.8.2 HTTPs over TR069

The TOE supports the use of a trusted channel (HTTPs) for user authentication and data transmission in TR069 remote management. Using HTTP or HTTPS depends on the ISP who deployed the ACS. However, the TOE supports setting the ACS server URL to use HTTPS only, and then the management traffic will be transferred through a security channel.

#### 7.1.8.3 WiFi Secure Channel

WiFi channel used WPA2 authentication and AES decryption is trusted. Usually, the product with WiFi AP feature uses WPA2+AES as the default configuration. A security risk notification will be prompted if unsecure authentication mode is used.

For wireless router (WSxxx), there is no WiFi authentication in default. When the user uses the device at first, he must configure the WiFi authentication password. The password complexity is indicated to inform the user its configuration is secure or not.

## 7.2 TOE Security Functions Rationale

| Security Functional Requirements | Security Functions |
|---|---|
| FAU_GEN.1 | F.Audit |
| FAU_GEN.2 | |
| FAU_SAR.1 | |
| FAU_SAR.3 | |
| FAU_STG.1 | |
| FAU_STG.3 | |
| FCS_COP.1(1)/AES,<br>FCS_CKM.1(1)/AES,<br>FCS_CKM.4(1)/AES | F.TSF_Protection |
| FCS_COP.1(2)/RSA,<br>FCS_CKM.1(2)/RSA,<br>FCS_CKM.4(2)/RSA | F.TSF_Protection |
| FCS_COP.1(3)/SHA256 | F.I&A<br>F.TSF_Protection |

| | |
|---|---|
| FDP_IFC.1 | F.UserDataProtection |
| FDP_IFF.1 | |
| FIA_AFL.1 | F.I&A |
| FIA_ATD.1 | |
| FIA_SOS.1 | |
| FIA_UAU.2 | |
| FIA_UID.2 | |
| FIA_UAU.6 | |
| FIA_UAU.7 | |
| FMT_MOF.1 | F.SecurityManagement |
| FMT_MSA.1 | |
| FMT_MSA.3 | |
| FMT_SMF.1 | |
| FMT_SMR.1 | |
| FPT_ITC.1 | F.TOE_Access |
| FPT_ITI.1 | |
| FPT_STM.1 | F.Audit |
| FTA_SSL.3 | F.TOE_Access |
| FTA_MCS.1 | |
| FTA_TSE.1 | |
| FTP_ITC.1 | F.TurstedPath/Channels |
| FTP_TRP.1 | |

**Table 8:** *TOE Security Functions Rationale*

# 8 Abbreviations

## 8.1 Abbreviations

| Abbreviation | Description |
|---|---|
| **ACL** | Access Control List |
| **ARP** | Address Resolution Protocol |
| **ATP** | Access Terminal Platform |
| **CC** | Common Criteria |
| **GUI** | Graphical User Interface |
| **SPI** | Stateful Packet Inspection |

| | |
|---|---|
| **RMT** | Remote Maintenance Terminal |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functions |
| **SNTP** | Simple Network Time protocol |