Security Target Huawei WLAN AP

Series Product

V200R007C10SPC200

Version: V0.8

Last Update: 2017-9-20

Developer: Huawei Technologies Co., Ltd

Revision record

Date	Revision Version	Change Description	Author
2016-11-04	0.1	Initial Draft	Ji Xiang
2016-11-18	0.2	Update by test result	Ji Xiang
2017-01-03	0.3	Update by test result	Chen Weiyi, Ji Xiang
2017-01-14	0.4	Updated by Comments	Chen Weiyi, Ji Xiang
2017-02-15	0.5	Updated by Review	Chen Weiyi
2017-03-13	0.6	Updated by Comments	Chen Weiyi
2017-03-31	0.7	Updated by Comments	Chen Weiyi
2017-09-20	0.8	Updated by Comments	Chen Weiyi

Table of Contents

List of Tables

1 Introduction

This Security Target is for the evaluation of the Huawei WLAN AP Series Product V200R007C10SPC200.

1.1 Security Target Reference

Name: CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target

Version: 0.8

Publication Date: 2017-09-20

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Reference

Name: Huawei WLAN AP Series Product

Version: V200R007C10SPC200

Developer name: Huawei Technologies Co., Ltd.

1.3 TOE Overview

At the core of Huawei WLAN AP Series Product is Versatile Routing Platform (VRP). TOE software version is V200R007C10SPC200. The TOE is a software TOE consisting of Huawei's Versatile Routing Platform supported by the Concurrence Accelerate Platform and the underlying OS as described in the following chapters.

1.3.1 TOE Type

The TOE is a WLAN Access Point (AP for networking functionality) system composed of a hardware platform and a software running within the platform as a whole system with the software as the TOE.

1.3.2 Usage and major security feature

Huawei WLAN AP Series Product is the product that provides 802.11-compliant wireless access for STAs to connect wired networks to wireless networks. The major security features provided by the TOE are:

Authentication: Authenticate administrative users by user name and password and AC devices using a pre-shared key.

Communication Security: Establishing a trusted path between itself and RMT and ACs is one of its features.

ACL: Access Control Lists (ACLs) to filter traffic destined to the TOE.

Security Management: Offers management functionality for its security functions.

1.3.3 Non-TOE hardware and software

Table 1-1 :Non-TOE hardware

Non-TOE hardware	Network: External networks or local networks with device(s) for the exchange of dynamic routing information (switches, routers).
	AC: Access Controller that manages and maintains the AP.
	AP: Access Pointer (Evaluated platforms see Table 1-2)
	Administrator: A personal computer that manages and maintains the AP.
Non-TOE software	NONE

Figure 1-1 Non-TOE hardware and software

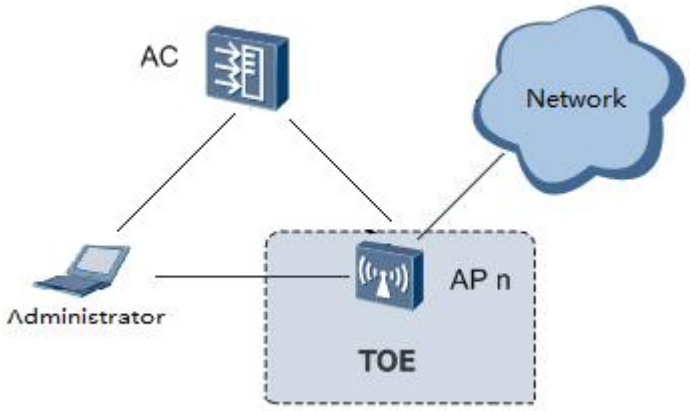


Table 1-2 : Evaluated Platforms

Name	CPU	MEMORY	FLASH	Description
AP4030DN	SOC QCA9557:1core@ 700M	256M DDR2, 32bit	32M NOR FLASH	The AP4030DN and AP4130DN hardware provides 802.11n/ac wireless access networks for places with simple building structure, small size, dense users, and high capacity demands, such as small and medium enterprises and
AP4130DN	SOC QCA9557:1core@ 700M	256M DDR2, 32bit	32M NOR FLASH	

Name	CPU	MEMORY	FLASH	Description
				branches. They can be flexibly deployed and work in both fit AP and bridge mode.
AP2030DN	SOC QCA9557:1core@ 700M	128M DDR2, 16bit	32M NOR FLASH	AP2030DN hardware offers both wired and wireless network connections, applicable to hotels, apartments, and offices.
AD9430DN-12	IPQ8068: ARM ,2core, 1.4GHz	1GB DDR3, 32bit	4M NOR FLASH +512MB NAND FLASH	The AD9430DN hardware is a central AP used in Huawei agile distributed Wi-Fi solution. It supports PoE power supply and can be connected to multiple remote units (RUs) deployed indoors. The central AP is recommended for environments with complex wall structures and high-density rooms, such as schools, hotels, hospitals, and office meeting rooms. AD9430DN-24: provides 24 downlink GE interfaces. AD9430DN-12: provides 12 downlink GE interfaces.
AD9430DN-24	CN6130: MIPS64, 4Core@1.1GHz	1GB DDR3, 64bit	16MB NOR FLASH + 2GB SD	
AP5030DN	SOC QCA9550:1core@ 700M	256M DDR2 32bit SDRAM	32M NOR FLASH	The AP5030D and AP5130DN hardware provides 802.11n/ac wireless access networks for places with simple building structure, small size, dense users, and high capacity demands, such as small and medium enterprises and branches. The AP5130DN hardware can be flexibly deployed and work in both fit AP and bridge mode.
AP5130DN	SOC QCA9550:1core@ 700M	256M DDR2 32bit SDRAM	32M NOR FLASH	

Name	CPU	MEMORY	FLASH	Description
AP8130DN	PPC P1025:2core@533 MHz	256MB DDR3 32bit SDRAM	64MB NOR FLASH	Huawei AP8130DNs hardware comply with IP67 dustproof and waterproof protection standards, applicable to coverage scenarios (for example, squares, pedestrian streets, and amusement parks) and bridging scenarios (for example, wireless harbors, data backhaul, video surveillance, and train-to-ground backhaul).
AP6050DN	IPQ8068: ARM ,2core, 1.4GHz	256MB DDR3L 32bit SDRAM	4M NOR FLASH +128MB NAND FLASH	The AP6050DN and AP6150DN hardware provide highest-quality wireless services for mobile office, high-density scenarios, elementary education, and higher education. They provide flexible distribution options in different environments.
AP6150DN	IPQ8068: ARM ,2core, 1.4GHz	256MB DDR3L 32bit SDRAM	4M NOR FLASH +128MB NAND FLASH	
AP7050DE	IPQ8068: ARM ,2core, 1.4GHz	512MB DDR3L 32bit SDRAM	4M NOR FLASH +128MB NAND FLASH	It provides high quality wireless services for large- and medium-sized enterprises in high-density scenarios, such as mobile office, elementary education, and higher education. The AP7050DE hardware provides flexible distribution options in different environments.

1.3.4 Excluded Functionality of the TOE

Features disabled by default that must remain disabled in the evaluated configuration:

The FTP protocol will bring risk to device security. The SFTP V2 mode is recommended. Ftp server is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.

The undo ftp server command disables the FTP server function so that FTP users cannot log in to the FTP server.

Telnet: Sends authentication data in plain text. This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target. The undo telnet server enable command stops a Telnet server.

1.4 TOE Description

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

1.4.1 Physical Scope

The TOE is delivered as software binaries that are downloaded from Huawei website at **http://e.huawei.com/uk/**. The binaries are different depending on the evaluated platform (Non-TOE hardware) where they are installed.

Name	FW and Version
AP4030DN	FitAP4X30XN_V200R007C10SPC200.bin
AP4130DN	FitAP4X30XN_V200R007C10SPC200.bin
AP2030DN	FitAP2X30XN_V200R007C10SPC200.bin
AD9430DN-12	FitAD9430DN-12_V200R007C10SPC200.bin
AD9430DN-24	FitAD9430DN-24_V200R007C10SPC200.bin
AP5030DN	FitAP5X30XN_V200R007C10SPC200.bin
AP5130DN	FitAP5X30XN_V200R007C10SPC200.bin
AP8130DN	FitAP8X30XN_V200R007C10SPC200.bin
AP6050DN	FitAP6050DN_V200R007C10SPC200.bin
AP6150DN	FitAP6150DN_V200R007C10SPC200.bin
AP7050DE	FitAP7050DE_V200R007C10SPC200.bin

These documents can be found in PDF format the CD provided in the product package upon delivery.

CC Huawei WLAN AP Series Product V200R007C10SPC200 Security Target	Version: 0.8
CC Huawei WLAN AP Series Product V200R007C10SPC200 Operational User Guidance	Version: 0.6
CC Huawei WLAN AP Series Product V200R007C10SPC200 Preparative Procedures for	Version: 0.5

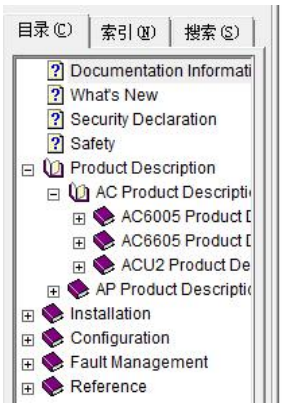
Production	

Additional guides (Product Documentation and Command Reference) are downloaded from the website http://support.huawei.com/enterprise/en/newindex.html by clicking on WLAN in Enterprise Networking in CHM format.

AC6605&AC6005&ACU2 (AC&FITAP) V200R007C10 Product Documentation	Product version 0.6
Huawei Access Points (FIT AP) V200R007C10 Command Reference	Issue 05

AC6605&AC6005&ACU2 (AC&FITAP) V200R007C10 Product Documentation and Huawei Access Points (FIT AP) V200R007C10 Command Reference also apply to the version V200R007C10SPC200.

Below is an example of the downloaded Product Document:



Documentation Information

This document helps you learn the documentation usage so that you can obtain required information efficiently and quickly.

If you want to...		Read...	
Task	**Sub-Task**	**Main Document**	**Reference Document**
Be familiar with the product.	Quickly know about product functions, hardware types, networking and application, and technical specifications.	Product Description	–
Install and commission the	Know safety precautions in hardware installation and maintenance.	Compliance and Safety Manual	–

1.4.2 Logical Scope

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

1. Authentication
2. ACL
3. Communication Security
4. Security Management

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs described within the security functional requirements as necessary to satisfy testing/assurance measures prescribed therein.

Authentication

User authentication is always enforced for virtual terminal sessions via SSH, and SFTP (Secured FTP) sessions. The use of SSH connection is always required for accessing the TOE via RMT.

Also, it authenticates AC devices in the network using pre-shared keys.

Communication Security

The TOE enforces communication security by implementing the SSH2 (SSH2.0) protocol for RMT. The trusted path provides data encryption, data integrity and authentication of both sides to protect the TOE from eavesdropping and to ensure data transmission security and confidentiality.

Beside SSH (which is sometimes also referred to as 'Secure Telnet' or 'STelnet') SFTP is provided implementing secure FTP based on SSH as communication protocol.

Also, DTLS v1.0 encryption provides a secure communication between the WLAN ACs deployed in the network and the TOE.

ACL

TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet), in order to provide controlled communications between two networks that are physically separated. When a packet flow reaches the TOE, the TOE applies an information flow security policy in the form of access control lists to the traffic before forwarding it into the remote network. Packet flows on Layer 3 arriving at a network interface of the TOE are checked to ensure that they conform the configured packet filter policy. For this, the TOE offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces.

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.

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.

Security functionality management

According to security functionality management, customized security is provided.

- The TSF shall be capable of performing the following management functions:
  1. Authentication, encryption policy

2. ACL policy.

1.4.3 Evaluated configuration

Configuration of TOE:

The TOE is a WLAN Access Point (AP) system composed of a hardware platform and a software running within the platform as a whole system with the software as the TOE.

Version of TOE: V200R007C10SPC200

Devices used during the evaluation:

Name
AP4030DN
AP4130DN
AP2030DN
AD9430DN-12
AD9430DN-24
AP5030DN
AP5130DN
AP8130DN
AP6050DN
AP6150DN
AP7050DE
Huawei AC6005 series and 6605 series that manage and maintain the AP.
A personal computer that manages and maintains the AP.

Documentation:

AC6605&AC6005&ACU2 (AC&FITAP) V200R007C10 Product Documentation	Product version 0.6
Huawei Access Points (FIT AP) V200R007C10 Command Reference	Issue 05

CC Huawei WLAN AP Series Product V200R007C10SPC200 Operational User Guidance	Version 0.5
CC Huawei WLAN AP Series Product V200R007C10SPC200 Preparative Procedures	Version 0.5

2 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. The CC version used is 3.1R4.

No conformance to a Protection Profile is claimed.

This ST is conforming to assurance package EAL2 without augmentations.

3 TOE Security problem definition

3.1 Threats

Threat Name	Threat Definition
T.UnauthenticatedAccess	A subject that is not an authenticated user of the TOE gains access to the TOE and modifies TOE configuration data without permission.
T.UnwantedNetworkTraffic	Any network user that sends unwanted/unexpected L3 network traffic to/through the TOE will reach resources on the network that it is not allowed to reach.
T. Eavesdroppping	An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets which are not protected against modification and disclosure that are exchanged between TOE and RMT and ACs.

3.2 Assumptions on the environment for the use of the TOE

Assumption Name	Assumption Definition
A.PhysicalProtection	It is assumed that the TOE (including any console attached, including any USB storage device attached) is protected against unauthorized physical access. The TOE is assumed not to contain any residual information that could be used for an attack when it is removed from the physically protected environment (e.g. for repair by a third party or at the end of life when the device is disposed).
A.NetworkElements	The environment is supposed to provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. These devices are: • Peer device(s) for the exchange of dynamic routing information; • Remote entities (PCs) used for administration of the TOE; • WLAN ACs intended to manage the TOE.
A.NoEvil	The authorized administrators are not careless, willfully negligent or hostile. They will follow and abide the instructions provided by the TOE documentation

4 Security Objectives

4.1 Objectives for the TOE

Object Name	Object Definition
O.Forwarding	The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds to a configured route for the destination IP address of the packet (L3 routing). The TOE shall provide Access Control List (ACL) functionality that can be configured to drop unwanted network traffic.

Object Name	Object Definition
O.Communication	The TOE must implement logical protection measures for network communication between the TOE and Remote Management Terminal (RMT) and WLAN ACs from the operational environment. These protection measures shall include device authentication and the use of a secure communication protocol.
O.Authentication	The TOE shall support the authentication of users by local username and password and using a pre-shared key. This applies to remote access (Remote Management Terminal) and WLAN ACs. The authentication mechanisms shall allow identifying users.
O.SecurityManagement	The TOE shall provide functionality to securely manage security functions provided by the TOE. This includes: • Authentication, encryption policy. • ACL policy.

4.2 Objectives for the Operational Environment

Object Name	Object Definition
OE.NetworkElements	The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. The operational environment shall provide network devices that the TOE needs to cooperate with: • Peer device(s) for the exchange of dynamic routing information; • AC for the management of AP devices; • Remote entities (PCs) used for administration of the TOE.
OE.Physical	The TOE (i.e., the complete system including attached peripherals, such as a console and USB mass storage devices) shall be protected against unauthorized physical access. Whenever the TOE is removed from the physically protected environment, it shall not contain any residual information that could be used for an attack.
OE.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE. This includes instruction to follow and abide the instructions provided by the TOE documentation.

4.3 Security Objectives Rationale

4.3.1 Coverage

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

Table 4-1 Mapping Objectives to Threats

Objective	Threat
O.Communication	T.Eavesdropping
O.Authentication	T.UnauthenticatedAccess
O.SecurityManagement	T.UnauthenticatedAccess T.Eavesdropping T.UnwantedNetworkTraffic
O.Forwarding	T.UnwantedNetworkTraffic

The following table provides a mapping of the objectives for the operational environment to assumptions and threats showing that each objective is at least covered by one assumption or threat.

Table 4-2 Mapping Objectives for the Environment to Threats, Assumptions

Environmental Objective	Threat / Assumption
OE.NetworkElements	A.NetworkElements
OE.Physical	A.PhysicalProtection
OE.Person	A.NoEvil

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 of that threat:

Table 4-3 Sufficiency analysis for threats

Threat	Rationale for security objectives to remove Threats
T.UnwantedNetworkTraffic	The TOE performs L3 forwarding of network traffic. ACL functionality can be used to deny unwanted L3 network traffic to enter or pass the TOE. (O.Forwarding) ACL functionality can be delivered by ACs intended to manage the AP. (O.SecurityManagement)
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). Authentication mechanisms can be configured (O.SecurityManagement).
T.Eavesdropping	The threat of eavesdropping is countered by requiring communication security via SSHv2 for communication between RMT and the TOE or DTLS for CAPWAP (O.Communication). Management of secure communication channels can be performed by users with sufficient user level (O.SecurityManagement).

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Table 4-4 Sufficiency analysis for assumptions

Assumption	Rationale for security objectives
A.NetworkElements	The assumption that the external environment provides securely and correctly working network devices such as peer device for routing information exchange, and management terminals for TOE control and management is addressed in OE.NetworkElements.
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access and that the TOE does not contain residual information that could be used for an attack whenever the TOE is removed from the physically protected environment is expressed by a corresponding requirement in OE.Physical.

Assumption	Rationale for security objectives
A.NoEvil	The assumption that the administrators of the TOE are not careless, willfully negligent, or hostile is addressed in OE.Person.

5 Extended Components Definition

There are no extended components defined for this security target.

6 Security Requirements

6.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ Indicates text removed as a refinement
- (Underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

6.2 TOE Security Functional Requirements

6.2.1 User Data Protection (FDP)

FDP_IFC.1 Subset information flow control

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

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

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

And operations: permit or deny access information.

FDP_IFF.1 Simple security attributes

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

Subjects security attributes:

- **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,**

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:

(a) **the information match the flow control policy;**

(b) **the flow control policy action is permitted;**

FDP_IFF.1.3 The TSF shall enforce the **following additional rules: none**.

FDP_IFF.1.4 The TSF shall explicitly authorise 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.**

6.2.2 Identification and Authentication (FIA)

FIA_AFL.1(a) Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **the session establishment**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met*,** the TSF shall **terminate the connection and close the session.**

FIA_AFL.1(b) Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **6** unsuccessful authentication attempts occur related to **the indicated user identity**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **block the user's account**.

FIA_ATD.1 User attribute definition

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

(a) **User ID**

(b) **Password**

(c) **Time when users are logging in.**

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.

FIA_UID.2 User identification before any action

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

6.2.3 Security Management (FMT)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **flow control policy** to restrict the ability to ***query, modify*** the security attributes **identified in FDP_IFF.1** to **role WLAN AC.**

FMT_MSA.3 Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the **role WLAN AC** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

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

(a) Authentication, encryption policy

(b) ACL policy.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Administrator**
- **WLAN AC**

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

6.2.4 TOE access (FTA)

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **time interval of user inactivity which can be configured by a user with sufficient user level.**

FTA_TSE.1 TOE session establishment

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

(a) **user authentication failure**

(b) **Source IP address**

6.2.5 Trusted Path/Channels (FTP)

FTP_TRP.1 Trusted path

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

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

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

6.3 Security Functional Requirements Rationale

6.3.1 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.

Table 6-1 Mapping SFRs to objectives

Security Functional Requirements	Objectives
FDP_IFC.1	O.Forwarding
FDP_IFF.1	O.Forwarding

Security Functional Requirements	Objectives
FIA_AFL.1(a) FIA_AFL.1(b)	O.Authentication
FIA_ATD.1	O.Authentication
FIA_UAU.2	O.Authentication
FIA_UID.2	O.Authentication
FMT_MSA.1	O.SecurityManagement
FMT_MSA.3	O.SecurityManagement
FMT_SMF.1	O.SecurityManagement
FMT_SMR.1	O.SecurityManagement
FTA_SSL.3	O.Communication
FTA_TSE.1	O.Communication
FTP_TRP.1	O.Authentication O.Communication

6.3.2 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 6-2 SFR sufficiency analysis

Security objectives	Rationale
O.Forwarding	FDP_IFC.1 and FDP_IFF.1 apply flow control policy to limit both packets going to the Control/Management Plane and through the TOE and thereby ensure that protected traffic goes through.
O.Communication	Communication security is implemented by the establishment of a trusted path for remote users in FTP_TRP.1. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1.

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 (a) and FIA_AFL.1 (b). User authentication via RMTs or ACs requires the use of a trusted path according to FTP_TRP.1.
O.SecurityManagement	Specification of Management Functions is covered in FMT_SMF.1. The definition of roles is provided by FMT_SMR.1. Requirements on the management functionality for the definition of flow control policy are provided in FMT_MSA.1 and FMT_MSA.3.

6.3.3 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:

Table 6-3 Dependencies between TOE Security Functional Requirements

Security Functional Requirement	Dependencies	Resolution
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FIA_AFL.1(a)	FIA_UAU.1	FIA_UAU.2
FIA_AFL.1(b)	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

Security Functional Requirement	Dependencies	Resolution
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	None	N/A
FTA_TSE.1	None	N/A
FTP_TRP.1	None	N/A

6.4 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.

6.5 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 Authentication

The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces. Detailed functions include:

(1) The TOE supports authentication via username and password.

(2) The TOE support authentication via pre-shared key previously established by a WLAN AC.

(3) The TOE stores the following security attributes for individual uses:

- User ID
- SHA256 Hashes of Passwords
- Time when users are logging in

(4) The TOE supports maximum number of authentication retries for an SSH connection. The default maximum number of authentication retries for an SSH connection is 3. The default maximum number of authentication retries before a user's account is blocked is 6.

(5) The TOE requires each user to be successfully authenticated before he can perform any other TSF-mediated actions except authentication according to 1) when connecting to the TOE.

(FIA_AFL.1(a), FIA_AFL.1(b), FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTP_TRP.1)

7.1.2 ACL

The TOE supports Access Control Lists (ACLs) to filter traffic destined to the TOE to prevent internal traffic overload and service interruption. And the TOE also uses ACLs to deny unwanted network traffic to pass through itself.

The TOE supports ACLs, which are based on the source and destination IP addresses, the source and destination port numbers.

(FDP_IFC.1, FDP_IFF.1)

7.1.3 Communication Security

The TOE provides two different trusted paths: CAPWAP using DTLS and SSH2.0.

- To establish the SSH trusted path, the SSH2.0 protocol shall be used. In addition, SFTP (i.e. FTP based on SSH protocol) is supported for secure file transfer. SSH communication is sometimes also referred to as STelnet.
- DTLS v1.0 is used to encrypt the CAPWAP communication between the TOE and WLAN AC.

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). STelnet based on the SSH protocol provides information security and authentication, which protects devices against attacks such as IP address spoofing.

(2) SFTP (i.e. FTP based on SSH protocol) is supported for file transfer.

(3) The TOE provides mechanisms to establish a trusted path between itself and a WLAN AC via pre-shared key previously established by an AC in order to encrypt the communication using DTLS.

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

(5) 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.

(6) The TOE supports termination of an interactive session after a given interval of user inactivity. This results in a loss of user authentication.

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

7.1.4 Security Management

The TOE offers management functionality for its security functions. Security management functionality can either be used through RMT using a SSH connection or a WLAN AC using a CAPWAP connection.

The security management functionality comprises:

1) Authentication, encryption policy: Users are allowed to configure the TOE to Authenticated administrative users by user name and password, configure a trusted path by encryption policies.

2) ACL policy: Users are allowed to configure Access Control Lists (ACLs) to filter traffic destined to the TOE.

ACL usually has 12-20 seconds delay after its deployment.

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

8 Abbreviations, Terminology and References

8.1 Abbreviations

AAA	Authentication Authorization Accounting
ACL	Access Control List
AM	Access Management
ARP	Address Resolution Protocol
CAP	Concurrence Accelerate Platform
CC	Common Criteria
CFM	Configuration Management
CLI	Command Line Interface
CM	Command Management
EXEC	Execute Command

AAA	Authentication Authorization Accounting
IC	Information Center
IM	Information Management
IPC	Inter-Process Communication
LMT	Local Maintenance Terminal
GUI	Graphical User Interface
MCU	Main Control Unit
MPU	Main Processing Unit
LPU	Line Process Unit
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SPU	Service Process Unit
SRU	Switch Router Unit
SSH	Secure Shell
ST	Security Target
STP	Spanning-Tree Protocol
TF	Traffic Forwarding
TOE	Target of Evaluation
TSF	TOE Security Functions
VRP	Versatile Routing Platform
VTY	Virtual Teletype Terminal
WLAN	Wireless Local Area Network

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator:	All the management users of the TOE using SSH (Administrators) or CAPWAP (WLAN AC) are considered no evil.
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.

8.3 References

[CC]	Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012, Version 3.1 Revision 4, CCMB-2012-09-001, -002, -003
[CEM]	Common Methodology for Information Technology Security Evaluation. Evaluation methodology, September 2012, Version 3.1 Revision 4, CCMB-2012-09-004
[PKCS#1 V2.1]	PKCS#1 V2.1: RSA Cryptography Standard, RSA Laboratories, Version 2.1, June, 2002
[PKCS#3]	PKCS#3: Diffie-Hellman Key-Agreement Standard, Version 1.4, November 1, 1993
[RFC 2104]	Request for Comments 2104, HMAC: Keyed-Hashing for Message Authentication, February 1997
[RFC 3526]	Request for Comments 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003
[RFC 4251]	Request for Comments 4251, The Secure Shell (SSH) Protocol Architecture, January 2006
[RFC 4252]	Request for Comments 4252, The Secure Shell (SSH) Authentication Protocol, January 2006
[RFC 4253]	Request for Comments 4253, The Secure Shell (SSH) Transport Layer Protocol, January 2006
[RFC 4254]	Request for Comments 4254, The Secure Shell (SSH) Connection Protocol, January 2006
RFC 4344]	Request for Comments 4344, The Secure Shell (SSH) Transport Layer Encryption Modes, January 2006
[RFC 4419]	Request for Comments 4419, Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, March 2006