Ruckus Solution

Security Target

Version 1.8

ISO 27001 Sertifisert
Sertifikat nr. 900364 I

ISO 9001 Sertifisert
Sertifikat nr. 900364

ISO 17025 Akkreditert

NTT Com Security (Norway) AS - www.nordics.nttcomsecurity.com

Office address: Havnegaarden – Kystveien 14 – 4841 Arendal
Postal address: Postboks 721 Stoa – 4808 Arendal
T +47 37 01 94 00

TABLE OF CONTENTS

List of Figures

List of Tables

ABBREVIATIONS

Abbreviation	Description
2RU's	2 Rack Units
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AD	Active Directory
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
CGF	Charging Gateway Function
CS	Circuit-Switched
CSV file	Comma-Separated Values
CTF	Charging Trigger Function
EAP	Extensible Authentication Protocol
EAP-AKA	EAP – Authentication and Key Agreement
EAP-SIM	EAP - Subscriber Identity Module
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled Transport Layer Security
EMS	Element Management System
EPC	Evolved Packet Core
FCAPS	Fault, Configuration, Accounting, Performance and Security
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
HetNet	Heterogeneous Network
HLR/HSS	Home Location Register / Home Subscriber Server
IMS	IP Multimedia Subsystem
ITU	International Mobile Telecommunications-2000 project of the International Telecommunication Union
JSON	JavaScript Object Notation
KPI	Key Performance Indicators
KVM	Kernel-based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTE	Long-Term Evolution
NAT	Network Address Translation
NMS	Network management System
NTP	Network Time Protocol
OSS/BSS	Operations Support Systems / Business Support Systems
PPPoE	Point-to-Point Protocol over Ethernet
PS	Packet-Switched
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBAC	Role-Based access Control
RESTful	Representational State Transfer
RF	Radio Frequency
SDN	Software Defined Networks
SIGTRAN	Signaling Transport
SIM	Subscriber Identity Module
SINR	Signal to Interference plus Noise Ratio
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

Abbreviation	Description
UAM	Universal Access Method
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access

DEFINITIONS

Definition	Description
3GPP	The 3rd Generation Partnership Project is collaboration between groups of telecommunications associations, known as the Organizational Partners. The initial scope of 3GPP was to make a globally applicable third-generation (3G) mobile phone system specification based on evolved GSM specifications within the scope of the ITU. The scope was later enlarged to include the development and maintenance of: • the GSM including GSM evolved radio access technologies • an evolved third Generation and beyond Mobile System based on the evolved 3GPP core networks, and the radio access technologies supported by the Partners • an evolved IMS developed in an access independent manner
802.11i	Standard for WLANs that provides improved encryption for networks that use the popular 802.11a, 802.11b (which includes Wi-Fi) and 802.11g standards. The 802.11i standard requires new encryption key protocols, known as TKIP and AES.
802.1X/EAP	The 802.1x standard is a security solution which can authenticate (identify) a user who wants to access a network (whether wired or wireless). This is done through the use of an authentication server. The 802.1x is based on the EAP protocol, used for transporting user identification information.
Backhaul	In a hierarchical telecommunications network the backhaul portion of the network comprises the intermediate links between the core network, or backbone network and the small sub networks at the "edge" of the entire hierarchical network. In contracts pertaining to such networks, backhaul is the obligation to carry packets to and from that global network.

Definition	Description
Captive portal	A captive portal is a special web page that is shown before using the Internet normally. The portal is often used to present a login page. This is done by intercepting most packets, regardless of address or port, until the user opens a browser and tries to access the web. At that time the browser is redirected to a web page which may require authentication and/or payment, or simply display an acceptable use policy and require the user to agree. Captive portals are used at many Wi-Fi hotspots, and can be used to control wired access (e.g. apartment houses, hotel rooms, business centers, "open" Ethernet jacks) as well.
Control and Data plane	The control plane is the part of a network that carries signaling traffic and is responsible for routing. Control packets originate from or are destined for a router. Functions of the control plane include system configuration and management. The data plane is the user data. Switching (packet forwarding) is performed in the data (forwarding) plane. Routing (exchange of routing information) is performed in the control plane. SDN is an approach to computer networking that allows network administrators to manage network services through abstraction of lower level functionality. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).
EAP	The EAP protocol is centered on the use of an access controller called an authenticator, which either grants or denies a user access to the network. The user in this system is called a supplicant. The access controller is a basic firewall which acts as an intermediary between the user and an authentication server, and requires very few resources to function. For a wireless network, the access point acts as the authenticator.
EAP-AKA	In UMTS based network, EAP-AKA authentication is implemented with a derived binding key function from the access network, typically a Universal Subscriber Identity Module (USIM). The AKA method is based on a challenge-response mechanism for mutual authentication. This limits the effects of compromised access network nodes and keys.
EAP-SIM	In a GSM-based network, the mobile node performs SIM authentication via the standard EAP Remote Access Dial-In User Service (RADIUS) protocol otherwise known as EAP-SIM. The same subscriber provisioning, authentication and service authorization inherits the already in place GSM services without changes to the mobile network elements.

Definition	Description
EAP-TLS	EAP-TLS is defined in RFC5216. The security of the Transport Layer Protocol (TLS) is strong, with the use PKI (public key infrastructure) to secure mutual authentication between the client to server and vice-versa. Both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust.
EAP-TTLS	Tunneled TLS EAP method (EAP-TTLS) is very similar to EAP-PEAP in the way it works. It does not require the client be authenticated to the server with a digitally signed certificate by the CA. The server uses the secure TLS tunnel to authenticate the client with password and key exchange mechanism.
EPC	EPC is a new, all-IP mobile core network for the LTE, specified by 3GPP standards. The EPC provides mobile core functionality that, in previous mobile generations (2G, 3G), has been realized through two separate sub-domains: CS for voice and PS for data. These two distinct mobile core sub-domains, used for separate processing and switching of mobile voice and data, are unified as a single IP domain. LTE will be end-to-end all-IP: from mobile handsets and other terminal devices with embedded IP capabilities, over IP-based Evolved NodeBs (LTE base stations), across the EPC and throughout the application domain (IMS and non-IMS). EPC is essential for end-to-end IP service delivery across LTE. As well, it is instrumental in allowing the introduction of new business models, such as partnering/revenue sharing with third-party content and application providers. EPC promotes the introduction of new innovative services and the enablement of new applications.
General-Purpose Computer	A device that manipulates data without detailed, step-by step control by human hand and is designed to be used for many different types of problems.
HetNet	A heterogeneous network is a network connecting computers and other devices with different operating systems and/or protocols. For example, local area networks (LANs) that connect Microsoft Windows and Linux based personal computers with Apple Macintosh computers are heterogeneous. The word heterogeneous network is also used in wireless networks using different access technologies. For example, a wireless network which provides a service through a wireless LAN and is able to maintain the service when switching to a cellular network is called a wireless heterogeneous network.
Hotspot	A hotspot is a site that offers Internet access over a wireless local area network (WLAN) through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi technology.

Definition	Description
HLR/HSS	The HSS is a database that contains user-related and subscriber-related information. It also provides support functions in mobility management, call and session setup, user authentication and access authorization. It is based on the pre-3GPP Release 4 - Home Location Register (HLR) and Authentication Centre (AuC).
LTE	Commonly marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is a converged framework for packet-based real-time and non-real-time services.
N+1 redundancy	N+1 redundancy is a form of resilience that ensures system availability in the event of component failure. Components (N) have at least one independent backup component (+1). The level of resilience is referred to as active/passive or standby as backup components do not actively participate within the system during normal operation. The level of transparency (disruption to system availability) during failover is dependent on a specific solution, though degradation to system resilience will occur during failover.
RADIUS	Networking protocol that provides centralized AAA management for users that connect and use a network service.
RAN	The range of a Wi-Fi computer network.
WISPr	Draft protocol that allows users to roam between wireless internet service providers, in a fashion similar to that used to allow cellphone users to roam between carriers. A RADIUS server is used to authenticate the subscriber's credentials. It covers best practices for authenticating users via 802.1X or the UAM, the latter being another name for browser-based login at a captive portal hotspot. It requires that RADIUS be used for AAA and defines the required RADIUS attributes.
WPA	Security technology for Wi-Fi networks, which provides strong data protection by using encryption as well as strong access controls and user authentication. WPA utilizes 128-bit encryption keys and dynamic session keys to ensure the wireless network's privacy and enterprise security.
WPA2 AES	WPA2 improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of the TKIP algorithm. All WPA2 networks use the AES, which uses a 128-bit block cipher to encrypt data that is sent and received over the Internet. ("WPA2" and "WPA2-AES" mean the same).
WPA-PSK	Authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.

Definition	Description
WPA-TKIP	TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks.

1. ST Introduction (ASE_INT)

1.1. ST and TOE References

The following table identifies the Security Target (ST).

Item	Identification
ST title	Ruckus Solution Security Target
ST version	See document log
ST author	NTT Com Security (Norway) AS

The following table identifies the Target of Evaluation (TOE).

Item	Identification
TOE name	Ruckus Solution
Deployment models	Distributed/Local-Breakout Deployment Model for SCG 200, SZ-100 and vSCG (Also known as vSZ-E and vSZ-H). Centralized Deployment Model for SCG 200 and SZ-100.
TOE identification	Wireless Controllers with RuckOS (formerly SCG) version 3.2.1: SCG 200, vSCG, SZ 100. Access Points: R310, R500, R600, R710, T300.

The following table identifies common references for the ST and the TOE.

Item	Identification
CC Version	3.1 Revision 4
Assurance level	EAL2 augmented with ALC_FLR.1
Protection Profile	None

1.2. TOE Introduction

The Ruckus Solution (TOE) is a Wireless LAN access system (WLAN). The Wireless LAN access system defined in this ST are multiple products operating together to provide secure wireless access to a wired and wireless network. The TOE provides end-to-end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement.

The TOE consists of minimum one wireless controller and minimum one access point from the following set.

- Wireless Controllers:
    - SmartCell Gateway 200 (SCG 200)
    - Virtual SmartCell Gateway (vSCG) (Also known as vSZ-E and vSZ-H)
    - Smart Zone 100 (SZ 100)
- Access Points:
    - ZoneFlex R310 Smart Wi-Fi Indoor (R310)
    - ZoneFlex R500 Smart Wi-Fi Indoor (R500)
    - ZoneFlex R600 Smart Wi-Fi Indoor (R600)
    - ZoneFlex R710 Smart Wi-Fi Indoor (R710)
    - ZoneFlex T300 Smart Wi-Fi Outdoor (T300)

RuckOS 3.2.1 runs on all Wireless Controllers (SCG 200, SZ 100, vSCG); of which SCG 200 and SZ 100 have the same high level application code but different hardware and drivers (low level code).

Non-TOE hardware/software required by the TOE for operation are the servers (RADIUS, Active Directory, Syslog, NTP, and SNMP).

The serial or console interface to the Ruckus AP is not included in the evaluated configuration of the TOE. This interface is not used for administration or configuration of the Ruckus AP component. All administration and configuration of the Ruckus AP component occurs through the Ruckus Wireless Controller component, which has CLI and HTTPS GUI interface for administration and configuration purpose.

1.3. TOE Overview

Ruckus Wireless Controller has been designed to eliminate the difficulties operators are experiencing with building and managing large-scale WLAN networks, to support several Wi-Fi access points and many concurrent Wi-Fi clients. It offers one of the industry's most scalable WLAN controller architectures, through a unique, dynamically scalable clustering model that maintains carrier-class availability and resiliency through N+1 redundancy and hot-swappable components. A cluster of Ruckus Wireless Controllers can support tens of thousands of Ruckus Smart Wi-Fi APs and hundreds of thousands of concurrent Wi-Fi subscribers, with an aggregate throughput of 20Gbps per 2RU's of rack space. The Ruckus carrier-class element management system can be integrated into an operator's central NMS via standard data exchange interfaces, providing feature-rich management of access points, such as RF management, load balancing, adaptive meshing and backhaul optimization.

1.3.1. Deployment Models

Ruckus Wireless Controllers and Ruckus Smart Wi-Fi Aps are deployed in two different models; distributed deployment model for SCG 200, SZ-100 and vSCG, and centralized deployment model for SCG 200 and SZ-100,

Distributed Deployment Model

In distributed deployment model client traffic directly reaches the intended destination. All Ruckus Wireless Controllers support this deployment model. See figure 1.

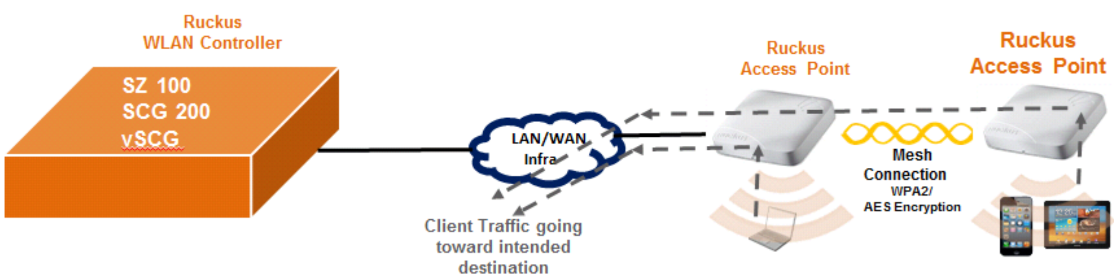

Figure 1: Distributed Deployment Model

Centralized Deployment Model

In centralized deployment model client traffic always reaches the WLAN controller first before going to intended destination. The Wireless Controller vSCG does not support this deployment model. See figure 2.

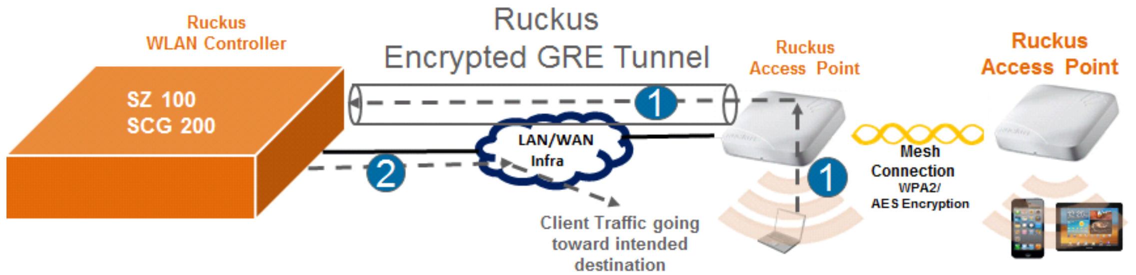

Figure 2: Centralized Deployment Model

1: Traffic sourced from a client traverses through tunnel to reach Ruckus Wireless Controller.
2: Ruckus Wireless Controller removes tunnel header, decrypts the packet and forwards the packet to network infrastructure to reach intended destination.

1.3.2. Ruckus Wireless Controllers

Ruckus Wireless Controller is comprised of different technology platforms based on scale and capacity, where the SmartCell Gateway 200 (SCG 200 or SZ-200) provides both WLAN controller and WLAN gateway functions at high scale, where the Smart Zone 100 (SZ 100) provides WLAN controller functions and WLAN gateway functions at smaller scale for enterprises, and where the Virtual SmartCell Gateway (vSCG) is a WLAN Controller designed to run in the cloud.

SmartCell Gateway 200

The SCG 200 can support both the WLAN Gateway and WLAN Controller functions running on the same platform at the same time, or these functions can run on separate platforms for maximum deployment flexibility. See figure 3.

Figure 3: SCG 200 System Overview

The SCG 200 provides both WLAN controller and WLAN gateway functions integrated into a single compact platform and managed as a single entity, which reduces the number of boxes that must be deployed and managed. The WLAN controller function can also be split out from the WLAN gateway function and they can run on separate platforms. The WLAN gateway can provide those functions locally and then offload traffic directly to the Internet.

SMART ZONE 100

SmartZone™ 100 (SZ 100) is the most Scalable, Resilient, and Highest Performing Wireless LAN controller within Ruckus family of WLAN controllers for Enterprises around the world. It manages up to 1,024 ZoneFlex Smart Wi-Fi access points, 2,000 WLANs, and 25,000 clients per device. Its RuckOS' unique architecture enables SZ 100 to be deployed in 3+1 Active-Active cluster. With Active-Active clustering all members (up to 4) of cluster will actively manage APs in the network and also provides the highest resiliency. With clustering it can manage up to 3,000 APs and 60,000 clients. Its Smart licensing allows customers to manage all the licensing needs online at https://Support.ruckuswireless.com. With Smart licensing, customers will have the ability to buy and assign licenses as granular as 1 (one) AP license.

VIRTUAL SMARTCELL GATEWAY

The vSCG is a scalable and versatile WLAN Controller designed to run in the cloud, and it is especially well suited to enabling a managed services offering. See figure 4.

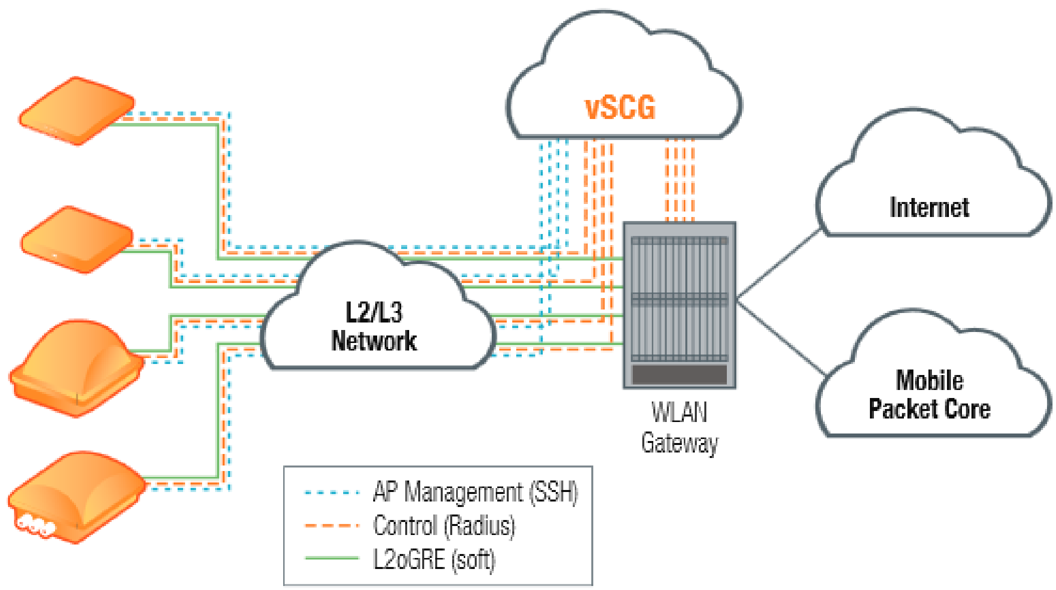

Figure 4: vSCG System Overview

Figure 4 shows how the vSCG would be deployed in an actual network[1]. All control plane traffic flows between the Ruckus access points and the vSCG in the cloud. All data plane traffic is routed directly from the Ruckus access points to a WLAN gateway, without passing through the vSCG. This greatly simplifies network design as it allows the WLAN Controller function to be consolidated in a national data center, while the WLAN gateway function can reside in regional data center. This approach allows client data to be quickly routed via the most expeditious path to the Internet. Ruckus supports L2oGRE (aka Soft GRE) for this data tunneling function. Soft GRE is supported by most WLAN gateways.

[1] The WLAN gateway shown in this figure is a 3rd party GRE concentrator. Hence, this will not be part of CC evaluation. Since L2oGRE is to establish a GRE tunnel from Ruckus AP to a 3rd party device this is not part of evaluation.

1.3.3. Ruckus Access Points

The access point provides the connection point between wireless client hosts and the wired network. Once authenticated as trusted nodes on the wired infrastructure, the access points provide the encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the wireless controller for management purposes. The management traffic between Ruckus AP and Ruckus Wireless Controller is encrypted using AES 128 bit SSH. See figure 5.

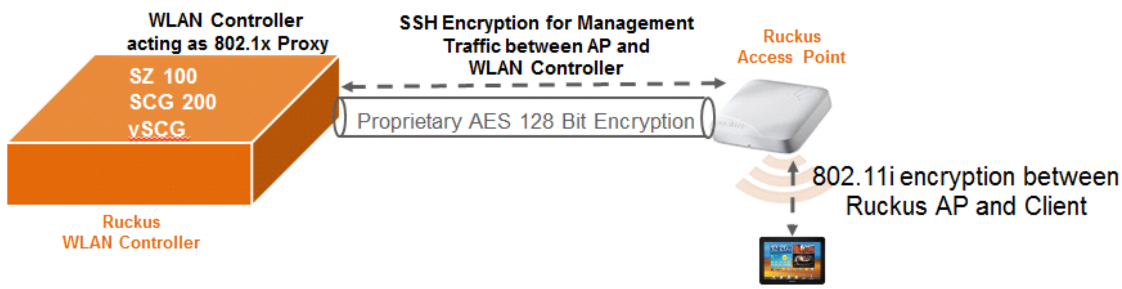

Figure 5: SSH Encryption between AP and Controller

The AP maintains a security domain for its own execution. The security domain is all the hardware and software that makes up the AP. The AP maintains the security domain by controlling the actions that can occur at the interfaces and providing the hardware resources that carry out the execution of tasks on the AP. Further, the AP provides for isolation of the different wireless clients that have sessions with the WLAN to include maintaining the keys necessary to support encrypted session with wireless devices.

By the AP controlling the actions and the manner external clients may interact with its external interfaces, the APs ensure that the enforcement functions of these components are invoked and succeed before allowing the external client to carry out any other mediate security function with or through the AP.

The APs have an RF interface and an Ethernet interface, and these interfaces are controlled by the software executing on the AP. The APs vary by the antenna support they offer, however the differences do not affect the security functionality claimed by the TOE.

1.3.4. Clients

The traffic between clients and Ruckus AP is encrypted using 802.11i (AES). See figure 6.

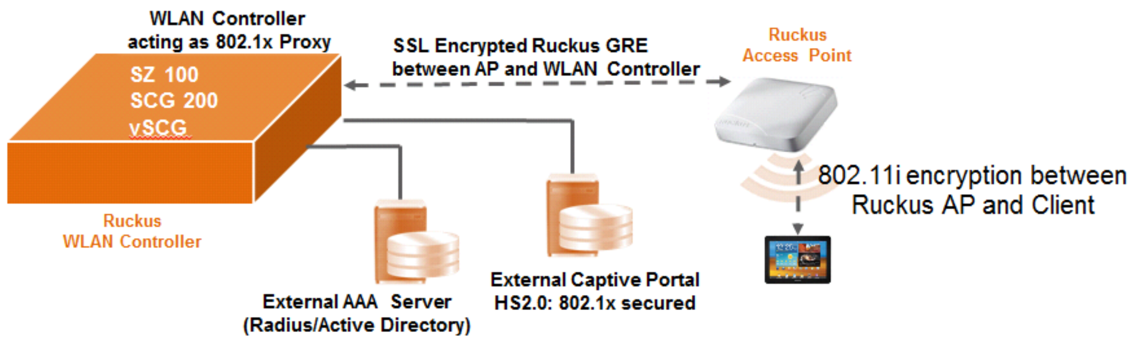

Figure 6: Client Authentication Process

1.4. TOE Description

The TOE is a system of products that are administratively configured to interoperate together to provide a WLAN. The TOE is meant to allow mobile or non-mobile, wireless clients to be roaming hosts on the wireless network, and to connect to the wired network using access points (APs). The TOE has the Access Point TOE components: Ruckus ZoneFlex Smart Wi-Fi R310, R500, R600, R710 Indoor Access Points, and T300 Outdoor Access Point; and the Wireless Controller TOE components: Ruckus SmartCell Gateway 200 (SCG 200 or SZ 200), Virtual SmartCell Gateway (vSCG or vSZ) and SZ 100 Wireless Controllers.

1.4.1. Wireless Controller

The wireless controller serves both SIM and non SIM-based client devices using carrier friendly authentication protocols, such as 802.1X/EAP. When this is combined with policy-based data traffic steering, operators can optimize the forwarding of all client traffic. When backhauling to the evolved packet core, the WLAN gateway function implements the Trusted WLAN Access approach, standardized by 3GPP. This utilizes 802.1x/EAP for authentication and 802.11i (AES) for airlink encryption, both of which are standard on today's smartphones.

The wireless controller can function as a very large-scale WLAN controller that can manage a lot of access points, providing feature-rich management including control over their self-organizing smart networking behaviors such as RF management, load balancing, adaptive meshing, and backhaul optimization. The following are some of the features that are enabled by the WLAN controller function:

- Seamless Low-Latency Wi-Fi Handoffs
    - Seamless handoff for clients as they move from one Wi-Fi AP to another in the coverage area. It is not necessary for the client to re-authenticate as they move about. Their credentials are passed from access point to access point.
- Hotspot 2.0
    - Seamless network discovery and selection along with seamless authentication using 802.1x/EAP. The Wi-Fi device will select the best available AP and begins the authentication process. This is automatic and requires no client intervention.
- Role-Based Access Control
    - The wireless controller's fully functional GUI provides concurrent RBAC for viewing the Wi-Fi system resources and performance. With the support of partitioning for access in a secure manner, the wireless controller allows

Wi-Fi service providers to give their managed services customers the ability to administer and monitor only the SSIDs over which they have control.

- Authentication support
  - Authentication support via EAP-SIM and EAP-AKA to the HLR/HSS client database in the evolved packet core, and also via traditional captive portal based login with ability to integrate to an external captive portal along with support for automatic portal based login via WISPr 1.0. See figure 7.
- Element Management System
  - With the built-in EMS, the wireless controller supports rapid deployment and eliminates the need for separate management systems. The built-in EMS provides client-friendly full-fledged FCAPS support and can be easily integrated with existing OSS/BSS systems via a variety of interfaces ranging from traditional CLI based interfaces to web programming friendly secure API based methods (RESTful JSON). See figure 8 and 9.

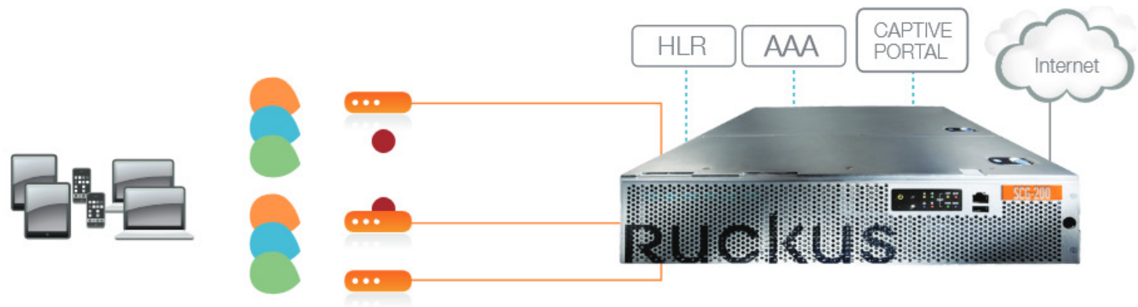

Figure 7: Authentication Support

Figure 7 shows that the wireless controller can authenticate subscribers with 802.1x/EAP authentication via EAP-SIM and EAP-AKA. Credentials can be passed to the HLR/HHS using either the SIGTRAN interface or an AAA server.

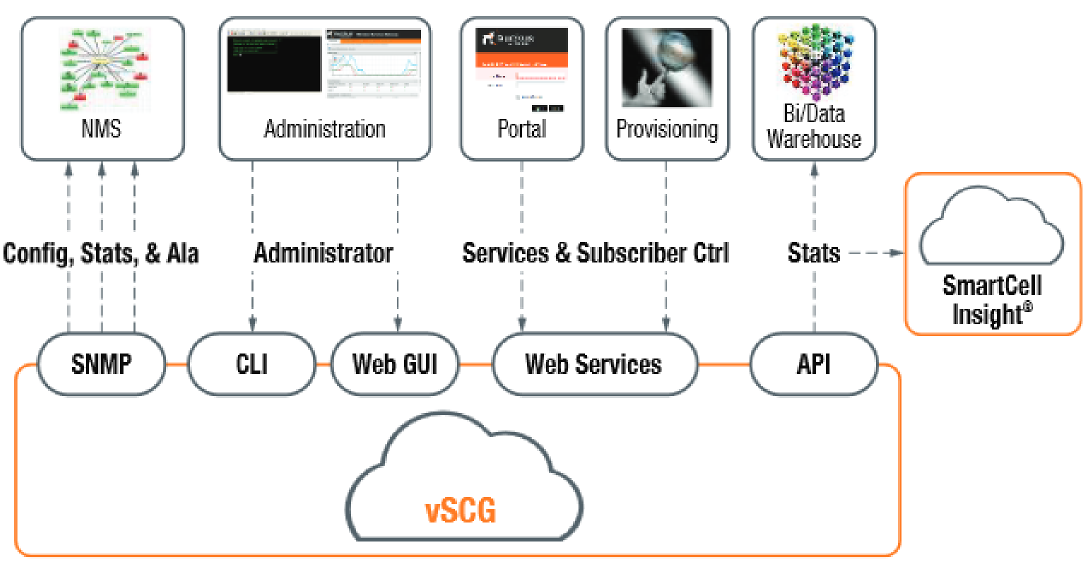

Figure 8: vSCG Operations and Administration

Figure 8 shows that the built-in EMS in the wireless controller (vSCG configuration) provides client-friendly full-fledged FCAPS support and can be easily integrated with existing OSS/BSS systems.

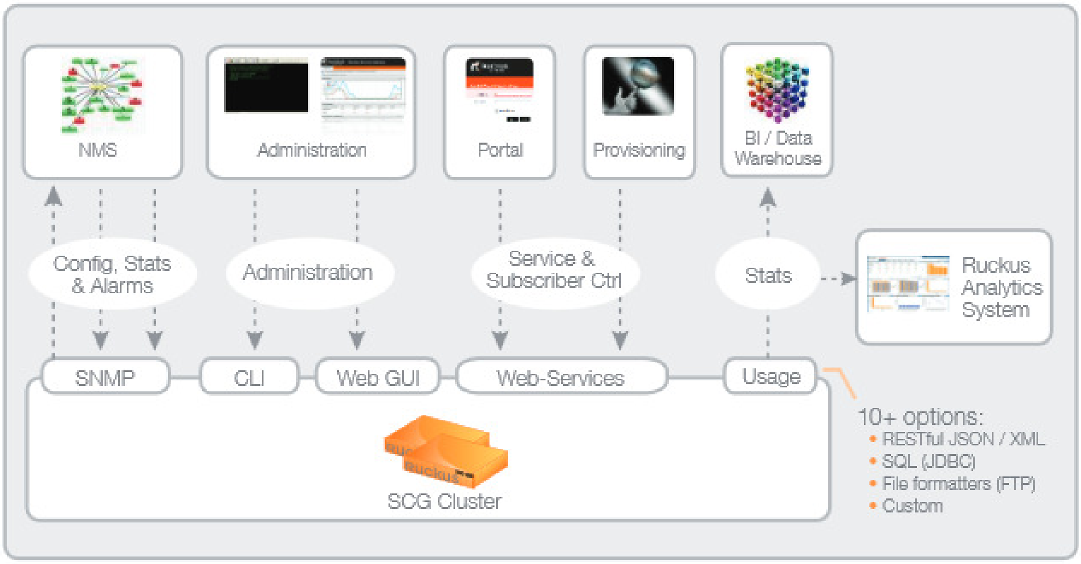

Figure 9: SCG 200 Operations and Administration

Figure 9 shows that the built-in EMS provides client-friendly full-fledged FCAPS support and can be easily integrated with existing OSS/BSS systems via a variety of interfaces ranging from traditional CLI based interfaces to web programming friendly secure API based methods (RESTful JSON).

SMARTCELL GATEWAY 200

The SCG 200 can provide the WLAN gateway function, which connects the Wi-Fi RAN to the Internet (or the evolved packet core). When offloading traffic to the Internet, the SCG 200 can provide all necessary services including authentication, address assignment, billing support, and more. It also allows operators to dynamically configure and manage network and client QoS/policy rules, in addition to being able to authorize, account and bill Wi-Fi clients. See figure 10.

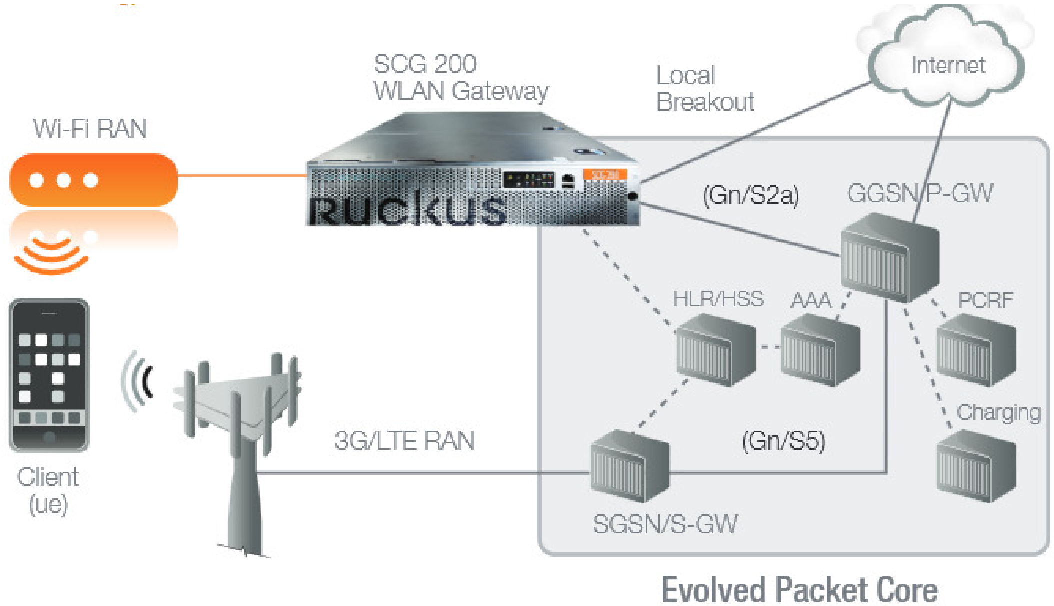

Figure 10: SCG 200 WLAN Gateway

The SCG 200 when operating as a WLAN Gateway, backhauls traffic to the evolved packet core using 3GPP trusted wireless LAN access. This approach enables a true HetNet experience where subscribers get the same services and the same experience regardless of the radio access technology.

The SCG 200 can support authentication via EAP-TLS (x.509 digital certificates) or EAP-TTLS (username and password). This enables a single point where network level vendor agnostic policy controls can be applied and KPIs can be generated.

Smart Zone 100

SmartZone™ 100 (SZ 100) is the most Scalable, Resilient, and Highest Performing Wireless LAN controller within Ruckus family of WLAN controllers for Enterprises around the world. It manages up to 1,024 ZoneFlex Smart Wi-Fi access points, 2,000 WLANs, and 25,000 clients per device. Its RuckOS' unique architecture enables SZ 100 to be deployed in 3+1 Active-Active cluster. With Active-Active clustering all members (up to 4) of cluster will actively manage APs in the network and also provides the highest resiliency. With clustering it can manage up to 3,000 APs and 60,000 clients. Its Smart licensing allows customers to manage all the licensing needs online at https://Support.ruckuswireless.com. With Smart licensing, customers will have the ability to buy and assign licenses as granular as 1 (one) AP license.

Virtual SmartCell Gateway (also known as vSZ-E and vSZ-H)

The vSCG is a scalable and versatile WLAN Controller designed to run in the cloud. By moving the SCG functionality into the cloud, it becomes possible to offer a platform with enormous scalability. The vSCG provides all control plane functions, with data plane traffic being routed directly from the APs to a separate WLAN gateway. This approach is consistent with the industry trend toward SDN that split out the control plane from the data plane.

Automatic Access Point Configuration is a process by which APs installed in the field can have their configuration automatically downloaded to them via the vSCG. See figure 11.

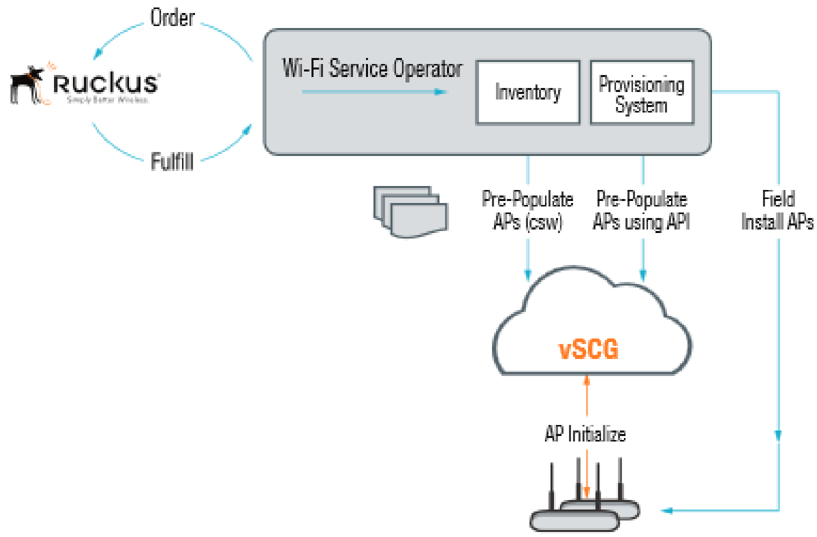

Figure 11: Automatic Access Point Configuration

Access point configuration is a key function of the vSCG and especially important when rolling out networks with tens of thousands or hundreds of thousands of access points. In a Ruckus network deployment, access points will automatically connect to a pre-determined vSCG instance when they are installed in the field. They will identify themselves via MAC address and serial number, and then their configuration will be automatically downloaded along with their zone number. The configuration information for each AP is downloaded to the vSCG from an external provisioning system via a CSV file or an API.

Virtualizing of the SCG is a key capability that will accelerate the deployment of managed WLAN services. It involves running the vSCG application and it's OS on top of either a KVM or a VMware vSphere hypervisor. See figure 12.

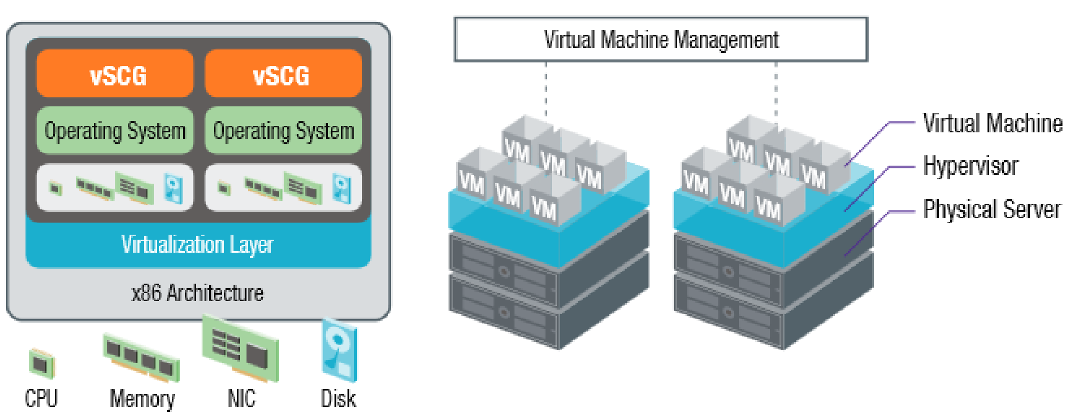

Figure 12: vSCG WLAN Controller Cloud design

The vSCG runs on a virtual machine established by the hypervisor, who in-turn runs atop the physical x86 blade servers. When deploying the vSCG in a data center, the existing cloud service management and orchestration function can interface with the vSCG through an API. This enables the rapid deployment of large numbers on managed WLAN networks in a cost effective manner.

1.4.2. Access point

The AP components can be centrally managed by the Ruckus Wireless Controller as part of a unified indoor/outdoor wireless LAN deployed as a standalone AP and managed individually. When used with the Ruckus WLAN controller, each AP supports a wide range of value-added applications such as guest networking and hotspot authentication. In a centrally managed configuration, the APs work with a wide range of authentication servers including AD and RADIUS.

Wireless communications between clients and APs is carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation the APs use a variation within 802.11a, 802.11ac, 802.11b, 802.11g and 802.11n for wireless communication. The wireless security protocols that are to be used with the APs are 802.1X/802.1i.

The AP components combines patented adaptive antenna technology and automatic interference mitigation to deliver consistent and predictable performance by means of BeamFlex, which is a software-controlled, high gain antenna array that continually forms and directs each 802.11n packet over the best performing signal path. The APs automatically select channels for highest throughput potential using ChannelFly dynamic channel management, adapting to environmental changes. ChannelFly uses actual activity to learn what channels will yield the most capacity to provide the highest client speeds and reduced interference, and selects automatically the best performing channel based on statistical, real-time capacity analysis of all RF channels.

The AP part of the TOE consists of five different component products:

- **ZoneFlex R310 Smart Wi-Fi Indoor** delivers high-performance and reliable wireless networking and combines patented adaptive antenna technology and automatic interference mitigation to deliver consistent, predictable performance.
- **ZoneFlex R500 Smart Wi-Fi Indoor** is purpose-built for enterprises requiring reliable high speed client connectivity. It is ideal for a variety of medium density enterprise and hotspot environments including SMBs, hotels, retail outlets and branch offices.
- **ZoneFlex R600 Smart Wi-Fi Indoor** is purpose-built for enterprises requiring reliable high speed client connectivity. It is ideal for a variety of medium density enterprise and hotspot environments including SMBs, hotels and schools.
- **ZoneFlex R710 Smart Wi-Fi Indoor** is purpose-built for high-capacity, high performance and interference-laden environments such as airports, public venues, hotels, universities and conference centers. Built for data-intensive streaming multimedia applications, for delivering of picture HD-quality IP video while supporting VoIP and data applications that have stringent quality of service requirements.
- **ZoneFlex T300 Smart Wi-Fi Outdoor** is designed explicitly for high density public venues such as airports, conventions centers, plazas & malls, and other dense urban environments. These environments require support for clients that demand high capacity and mobile device ready WLAN services.

Non-TOE hardware/software required by the TOE for operation are the servers (RADIUS, Active Directory, Syslog, NTP, and SNMP).

1.4.3. Evaluated Configuration

- Evaluated configuration:
  - Distributed and Centralized Deployment models
  - 802.1X/11i Encrypted Tunnels
  - External AAA Server and Captive Portal

- Not covered as part of the evaluation configuration:
  - 3rd Party APs
  - 3rd Party Soft-GRE Concentrator
  - External Syslog, NTP, SNMP servers
  - Built-in Captive Portals
  - GTP Tunnel (North of SCG)

1.5. Notations and Formatting

The notations and formatting used in this ST are consistent with version 3.1 Revision 4 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, [**Assignment_value**].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.User. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.Crypto_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

2. CC Conformance Claim (ASE_CCL)

This TOE and ST are conformant with the following specifications.

Item	Identification
CC Part 2	Security functional components, September 2012, Version 3.1, Revision 4, conformant
CC Part 3	Security assurance components, September 2012, Version 3.1, Revision 4, conformant, EAL2 augmented with ALC_FLR.1
Assurance level	EAL2 augmented with ALC_FLR.1
Protection Profile	None
Extended SFRs	None

3. Security Problem Definition (ASE_SPD)

3.1. Threats to security

3.1.1. Assets

Assets	Description
AS.SECURE_ COMMUNICATION_ CHANNEL	Client service Availability: Secure WLAN communication channel between client and services, through the TOE.
AS.INFO	Client information/data through secure WLAN communication channel.
AS.CLIENT_ ACCREDITATIONS	Client ID, client password, client cryptographic key, client certificate.

3.1.2. Threat Agents

Threat Agents	Description
TA.ADMIN	Authorized person/process that performs installation/updates and configuration/setup of the TOE to ensure that the TOE operates according to clients' needs.
TA.ATTACKER	A person/company or process with skills and resources to mislead the system in any way necessary to misuse client services and prevent the system from operating.
TA.CLIENT	Wi-Fi device client/process may perform unintentional unauthorized actions; or perform an authorized action, but unintentionally receive data not relevant to their request/response.

3.1.3. Identification of Threats

3.1.3.1. Threats to the TOE

Threats to the TOE	**Description**
TT.ADMIN_ERROR	The TOE may be incorrectly configured that may result in the TOE's acquisition of ineffective security mechanisms.
Threat agent:	TA.ADMIN
Assets:	AS.SECURE_COMMUNICATION_CHANNEL and AS.INFO
Attack method:	During operation, the administrator unintentionally configures the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.
TT.ADMIN_EXPLOIT	A person/company may gain access to an administrator account.
Threat agent:	TA.ATTACKER
Assets:	AS.SECURE_COMMUNICATION_CHANNEL, AS.INFO and AS.CLIENT_ACCREDITATIONS
Attack method:	A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.

Threats to the TOE	Description
TT.CRYPTO_ COMPROMISE	An attacker may compromise the cryptographic key and the data protected by the cryptographic mechanisms.
Threat agent:	TA.ATTACKER
Assets:	AS.INFO and AS.CLIENT_ACCREDITATIONS
Attack method:	An attacker cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
TT.EAVESDROPPING	Eavesdropping of the communication between clients and access points. This includes man-in-the-middle, side-channel, or other redirection attacks.
Threat agent:	TA.ATTACKER
Assets:	AS.INFO and AS.CLIENT_ACCREDITATIONS
Attack method:	An unauthorized person with no physical access to TOE is eavesdropping on the communication between Wi-Fi clients and access points to intercept client data.
TT.EXPLOIT_VULN	A person/company tries to exploit vulnerability in the TOE to get unauthorized access to TOE resources.
Threat agent:	TA.ATTACKER
Assets:	AS.SECURE_COMMUNICATION_CHANNEL
Attack method:	A person/company uses hacking methods to exploit weakness in the TOE.
TT.HACK_ACCESS	A person/company gets undetected system access to the TOE due to missing, weak and/or incorrectly implemented access control, causing potential violations of integrity, confidentiality or availability.
Threat agent:	TA.ATTACKER
Assets:	AS.SECURE_COMMUNICATION_CHANNEL and AS.INFO
Attack method:	A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.
TT.MALFUNCTION	The TOE may malfunction which may compromise data or TOE resources.
Threat agent:	TA.ATTACKER or TA.CLIENT
Assets:	AS.SECURE_COMMUNICATION_CHANNEL, AS.INFO and AS. CLIENT _ACCREDITATIONS
Attack method:	The TOE may malfunction which may compromise data or TOE resources.
TT.RESIDUAL_DATA	Incorrect reallocation of TOE resources
Threat agent:	TA. CLIENT
Assets:	AS.INFO and AS. CLIENT_ACCREDITATIONS
Attack method:	A client or process may gain unauthorized access to data through reallocation of TOE resources from one client or process to another.
TT.SPOOFING	The TOE may be subject to spoofing attack that may compromise data or TOE resources.
Threat agent:	TA.ATTACKER
Assets:	AS.INFO and AS. CLIENT _ACCREDITATIONS

Threats to the TOE	Description
Attack method:	An attacker masquerades as another entity in order to gain unauthorized access to data or TOE resources.
TT.TAMPERING	The TOE may be subject to physical attack that may compromise TOE resources.
Threat agent:	TA.ATTACKER
Assets:	AS.SECURE_COMMUNICATION_CHANNEL
Attack method:	A person/company tampers with wireless controllers or access points to get hold of TOE services and configuration accessibilities.
TT.UNATTENDED_ CONTROL_PLANE	The TOE may be subject to a control plane attack that may compromise TOE resources.
Threat agent:	TA.ATTACKER
Assets:	AS.SECURE_COMMUNICATION_CHANNEL
Attack method:	An attacker may gain unauthorized access to an unattended control plane session to get hold of TOE services and configuration accessibilities.

3.1.3.2. Threats to the TOE environment

Threats to the TOE environment	Description
TE.ADMIN_FAIL	The administrator fails to perform functions essential to the security.
Threat agent:	TA.ADMIN
Assets:	AS.SECURE_COMMUNICATION_CHANNEL and AS.INFO
Attack method:	The administrator fails to or forgets to update the TOE with security patches.
TE.STOLEN_MOBILE_ ENTITY	A stolen mobile entity with ongoing secure WLAN communication channel between client and services, through the TOE.
Threat agent:	TA.ATTACKER
Assets:	AS.INFO
Attack method:	An attacker steals a client mobile entity (e.g. phone/tablet/laptop) to exploit an ongoing secure WLAN communication channel between client and services, through the TOE.

3.2. Organizational security Policies

Organizational security Policies	Description
P.ACCOUNTABILITY	The administrators of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.

Organizational security Policies	Description
P.ENTITY	The TOE shall utilize 802.1x/EAP for authentication and 802.11i (AES) for airlink encryption, both of which are standard on mobile devices (e.g. phone/tablet/laptop).
P.NO_GENERAL_ PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g. compilers/editors/user applications) available on the TOE.
P.PATCH	The patch policy for the TOE must be sufficient to stop all known, publicly available vulnerabilities in the TOE software.
P.SOFTWARE	All installations of and changes to TOE software shall be done by an administrator, following strict change control and configuration management processes and procedures.

3.3. Assumptions

Assumptions	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	The administrators of the TOE will not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

4. Security objectives (ASE_OBJ)

4.1. TOE Security Objectives

Security Objectives	Description
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.CORRECT_TSF_OPERERATION	The TOE will provide the capability to verify the correct operation of the TSF.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and the integrity of client data that is transmitted on the air.
O.INTEGRITY	The TOE must ensure the integrity of all audit and system data.
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.

4.2. Operational Environment Security Objectives

Security Objectives	Description
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g. compilers/editors/user applications) available on the TOE.
OE.PHYSICAL	The environment provides physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

4.3. Security Objectives Rationale

Threats/ Policies/ Assumptions Objectives	TT.ADMIN_ERROR	TT.ADMIN_EXPLOIT	TT.CRYPTO_COMPROMISE	TT.EAVESDROPPING	TT.EXPLOIT_VULN	TT.HACK_ACCESS	TT.MALFUNCTION	TT.RESIDUAL_DATA	TT.SPOOFING	TT.TAMPERING	TT.UNATTENDED_CONTROL_PLANE	TE.ADMIN_FAIL	TE.STOLEN_MOBILE_ENTITY	P.ACCOUNTABILITY	P.CRYPTOGRAPHIC	P.ENCRYPTED_CHANNEL	P.ENTITY	P.NO_GENERAL_PURPOSE	P.PATCH	P.SOFTWARE	A.PHYSICAL	A.TRUSTED_ADMIN
TOE Security Objectives																						
O.AUDIT_ GENERATION						X	X			X			X	X								
O.CORRECT_ TSF_OPERATION							X															
O.CRYPTO-GRAPHY				X			X			X					X	X	X					
O.INTEGRITY						X	X															
O.MANAGE	X	X		X	X	X						X		X					X	X		
O.MEDIATE				X		X										X	X					
O.RESIDUAL_ INFORMATION			X					X							X							
O.SELF_ PROTECTION			X		X	X	X			X			X									
O.TOE_ ACCESS		X				X	X		X		X		X	X								
Operational Environment Security Objectives																						
OE.NO_ GENERAL_ PURPOSE	X																	X				
OE.PHYSICAL										X											X	
OE.TRUSTED_ ADMIN	X	X			X	X						X							X	X		X

Table 1: Mapping of Objectives to Threats, Policies and Assumptions

Threat/Policy/Assumption	Security Objective Rationale
TT.ADMIN_ERROR	O.MANAGE provides administrators the capability to view and manage configuration settings. For example, if the administrator made a mistake when configuring the set of permitted clients' authentication credentials, providing them the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made. OE.NO_GENERAL_PURPOSE ensures that there can be no accidental errors by providing that there are no general-purpose or storage repository applications available on the TOE. OE.TRUSTED_ADMIN ensures that the administrators are non-hostile

	and are trained to appropriately manage and administer the TOE.
TT.ADMIN_EXPLOIT	O.MANAGE restricts access to administrative functions and management of TSF data to the administrator. O.TOE_ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions. OE.TRUSTED_ADMIN ensures the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
TT.CRYPTO_ COMPROMISE	O.RESIDUAL_INFORMATION ensures that any residual data is removed from network packet objects and ensure that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked.
TT.EAVESDROPPING	O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality and integrity protection of client data that is transmitted on the air. O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. O.MEDIATE allows the TOE administrator to set a policy to encrypt all wireless traffic.
TT.EXPLOIT_VULN	O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.TRUSTED_ADMIN ensures the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
TT.HACK_ACCESS	O.AUDIT_GENERATION provides the TOE the capability to detect and create records of security-relevant events associated with users. O.INTEGRITY ensures the integrity of all audit and system data. O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy. O.MEDIATE ensures that all network packets that flow through the TOE are subject to the information flow policies. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. O.TOE_ACCESS includes mechanisms to authenticate TOE clients and place controls on client sessions. OE.TRUSTED_ADMIN ensures the TOE administrators have guidance

	that instructs them how to administer the TOE in a secure manner.
TT.MALFUNCTION	O.AUDIT_GENERATION provides the TOE the capability to detect and create records of security-relevant events associated with users. O.CORRECT_TSF_OPERERATION ensures that users can verify the continued correct operation of the TOE after it has been installed in its target environment. O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality and integrity protection of client data that is transmitted on the air. O.INTEGRITY ensures the integrity of all audit and system data. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. O.TOE_ACCESS includes mechanisms to authenticate TOE clients and place controls on client sessions.
TT.RESIDUAL_DATA	O.RESIDUAL_INFORMATION ensures that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.
TT.SPOOFING	O.TOE_ACCESS controls the logical access to the TOE and its resources. By constraining how and when authorized clients can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a client attempting to login and masquerade as an authorized client. In addition, this objective provides the administrator the means to control the number of failed login attempts a client can generate before an account is locked out, further reducing the possibility of a client gaining unauthorized access to the TOE. The TOE includes requirements that ensure protected channels are used to authenticate wireless clients and to communicate with critical portions of the TOE IT environment.
TT.TAMPERING	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users. O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality and integrity protection of client data that is transmitted on the air. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.PHYSICAL Ensures that the environment provides physical security, commensurate with the value of the TOE and the data it contains.
TT.UNATTENDED_ CONTROL_PLANE	O.TOE_ACCESS includes mechanisms that place controls on control planes sessions. The sessions are dropped after a defined time period of inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the TOE device where the session was established, thus gaining unauthorized access to the session.
TE.ADMIN_FAIL	O.MANAGE provides administrators the capability to update the TOE

	with security patches. OE.TRUSTED_ADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
TE.STOLEN_MOBILE_ ENTITY	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. O.TOE_ACCESS includes mechanisms that place controls on sessions. The sessions are dropped after a defined time period of inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the mobile device for which the session was established, thus gaining unauthorized access to the session.
P.ACCOUNTABILITY	O.AUDIT_GENERATION provides the administrator with the capability of configuring the audit mechanism to record the actions for a specific event type, or review the audit trail based on event type, date and time.. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted path, etc.). O.MANAGE ensures that access to administrative functions and management of TSF data is restricted to the administrator. O.TOE_ACCESS controls logical access to the TOE and its resources. These objectives ensure that users are identified and authenticated so that their actions may be tracked by the administrator.
P.CRYPTOGRAPHIC	O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality and integrity protection of client data that is transmitted on the air. O.RESIDUAL_INFORMATION ensures that cryptographic data is cleared according to the cryptographic services.
P.ENCRYPTED_ CHANNEL	O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality and integrity protection of client data while in transit for wireless clients that are authorized to join the network. O.MEDIATE allows the TOE administrator to set a policy to encrypt all wireless traffic.
P.ENTITY	O.MEDIATE ensures that all network packets that flow through the TOE are subject to the information flow policies. O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality and integrity protection of client data that is transmitted on the air.
P.NO_GENERAL_ PURPOSE	OE.NO_GENERAL_PURPOSE ensures that there are no general-purpose computing or storage repository capabilities (e.g. compilers/editors/user applications) available on the TOE.
P.PATCH	O.MANAGE ensures that the TOE will provide functions and facilities necessary to support the administrators in their management of the security

	of the TOE. OE.TRUSTED_ADMIN ensures that the administrators are trained to appropriately manage and administer the TOE.
P.SOFTWARE	O.MANAGE ensures that the TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.TRUSTED_ADMIN ensures that the administrators are trained to appropriately manage and administer the TOE.
A.PHYSICAL	OE.PHYSICAL Ensures that the environment provides physical security, commensurate with the value of the TOE and the data it contains.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN ensures that the administrators of the TOE will not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

Table 2: Rationale between Objectives and SPD

5. Extended Components Definition (ASE_ECD)

Not applicable.

6. Security requirements (ASE_REQ)

6.1. Security Functional Requirements (SFRs)

Functional Class	Functional Component	
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
FDP: User data protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_RIP.1	Subset residual information protection
FIA: Identification and authentication	FIA_ATD.1(1)	Administrator attribute definition
	FIA_ATD.1(2)	Client attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.2	User identification before any action
FMT: Security management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing

Functional Class	Functional Component	
FTA: TOE access	FTA_SSL.3	TSF-Initiated termination
FTP: Trusted path/channels	FTP_TRP.1	Trusted path

Table 3: Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [**TOE security events**].

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, [**None**].

6.1.1.2. FAU_GEN.2 User identity association

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

6.1.1.3. FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**Wireless Controller administrators**] with the capability to read [**all audit 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.

6.1.1.4. FAU_SAR.2 Restricted audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5. FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches, sorting, ordering**] of audit data based on [**event type, date, time, none**].

6.1.1.6. FAU_SEL.1 Selective audit

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:
a) [*event type*]
b) [**None**]

6.1.2. Cryptographic Support (FCS)

6.1.2.1. FCS_CKM.1 Cryptographic key generation

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[random generator]** and specified cryptographic key sizes **[128-bit]** that meet the following: **[FIPS PUB 197]**.

6.1.2.2. FCS_CKM.4 Cryptographic key destruction

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[key zeroization in RAM]** that meets the following: **[none]**.

6.1.2.3. FCS_COP.1 Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform **[encryption/decryption]** in accordance with a specified cryptographic algorithm **[AES]** and cryptographic key sizes **[128-bit]** that meet the following: **[FIPS PUB 197]**.

6.1.3. User Data Protection (FDP)

6.1.3.1. FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [**WLAN information flow control SFP**] on [**subjects: wireless clients that send information through the TOE interface, information: network packets, operations: send**].

6.1.3.2. FDP_IFF.1 Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [**WLAN information flow control SFP**] based on the following types of subject and information security attributes: [**subject security attributes: IP address of wireless client**; **information security attributes: source IP, destination IP, destination port**].

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: [**no additional information flow control SFP rules**].

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional information flow control SFP rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no additional information flow control SFP rules**].

6.1.3.3. FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to/deallocation of the resource from*] the following objects: [**network packet objects**].

Application Note (for deallocation): This requirement ensures that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet.

6.1.4. Identification and Authentication (FIA)

6.1.4.1. FIA_ATD.1(1) Administrator attribute definition

Dependences: None.

FIA_ATD.1.1 (1) Refinement: The TSF shall maintain the following list of security attributes belonging to individual **administrators**: [**username, password, role**].

6.1.4.2. FIA_ATD.1(2) Client attribute definition

Dependences: None.

FIA_ATD.1.1 (2) Refinement: The TSF shall maintain the following list of security attributes belonging to individual **remotely authenticated wireless clients**: [**client ID, client cryptographic key**].

6.1.4.3. FIA_UAU.1 Timing of authentication

Dependences: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [**admin/client identification as stated in FIA_UID.2**] on behalf of the user to be performed before the user is authenticated.

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

6.1.4.4. FIA_UID.2 User identification before any action

Dependencies: None.

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.

6.1.5. Security management (FMT)

6.1.5.1. FMT_MOF.1 Management of security functions behaviour

Dependences: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to [*enable*] the functions **[generating of reports based on subscriber's statistics]** to **[Wireless Controller administrators]**.

6.1.5.2. FMT_MSA.1 Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**WLAN information flow control SFP**] to restrict the ability to [*modify*] the security attributes [**referenced in the FDP_IFF.1**] to [**Wireless Controller administrators**].

6.1.5.3. FMT_MSA.2 Secure security attributes

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [**security attributes referenced in the FDP_IFF.1**].

6.1.5.4. FMT_MSA.3 Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**WLAN information flow control SFP**] to provide [*permisive*] default values for security attributes that are used to enforce the SFP.

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

6.1.5.5. FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*query*] the [**audit trail**] to [**Wireless Controller administrators**].

6.1.5.6. FMT_SMF.1 Specification of Management Functions

Dependencies: None.

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

- **SW installation/updates of the TOE**
- **configuration/setup of the TOE**
- **configuration audit trails**].

6.1.5.7. FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **[Wireless Controller administrator roles, wireless client]**.

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

6.1.6. Protection of the TSF (FPT)

6.1.6.1. FPT_ITT.1 Basic internal TSF data transfer protection

Dependencies: None.

FPT_ITT.1.1 The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

6.1.6.2. FPT_STM.1 Reliable time stamps

Dependencies: None.

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

6.1.6.3. FPT_TST.1 TSF testing

Dependencies: None.

FPT_TST.1.1 The TSF shall run a suite of self tests [*during initial start-up, at the conditions* [***upon request***]] to demonstrate the correct operation of [*the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [*TSF data*].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [*TSF*].

6.1.7. TOE ACCESS (FTA)

6.1.7.1. FTA_SSL.3 TSF-INITIATED TERMINATION

Dependencies: None.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**Wireless Controller administrator configurable time interval of client inactivity**].

6.1.8. TRUSTED PATH/CHANNELS (FTP)

6.1.8.1. FTP_TRP.1 TRUSTED PATH

Dependencies: None.

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*, [***replay***]].

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 [[***wireless client authentication, remote TOE administration]***]].

6.2. SECURITY ASSURANCE REQUIREMENTS (SARS)

The assurance level of the TOE is EAL2 augmented with ALC_FLR.1.

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
	ALC_FLR.1 Basic flaw Remediation
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

Table 4: Assurance requirements

6.3. Security Requirements Rationale

6.3.1. Relation between SFRs and security objectives

Requirements / Objectives	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_SEL.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_IFC.1	FDP_IFF.1	FDP_RIP.1	FIA_ATD.1(1)	FIA_ATD.1(2)	FIA_UAU.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_ITT.1	FPT_STM.1	FPT_TST.1	FTA_SSL.3	FTP_TRP.1
O.AUDIT_GENERATION	X	X	X	X	X	X																			X			
O.CORRECT_TSF_ OPERATION																										X		
O.CRYPTOGRAPHY							X	X	X																			
O.INTEGRITY																						X		X				
O.MANAGE																	X	X	X	X	X	X	X					
O.MEDIATE										X	X				X	X												
O.RESIDUAL_ INFORMATION								X				X																
O.SELF_PROTECTION																								X				
O.TOE_ACCESS													X	X	X	X											X	X

Table 5: Tracing of functional requirements to Objectives

Security Objective (TOE)	Security Functional Requirement Rationale
O.AUDIT_GENERATION	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SAR.1 ensures that the TOE provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.2 restricts the ability to read the audit records to only the administrator. FAU_SAR.3 provides the administrator with the ability to selectively review the contents of the audit trail based on established criteria. This capability allows the administrator to focus their audit review to what is pertinent at that time. FAU_SEL.1 allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the event type can be used as selection criteria for the events to

	be audited. FPT_STM.1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events.
O.CORRECT_TSF_ OPERATION	FPT_TST.1 is necessary to ensure the correct operation of the TSF. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies.
O.CRYPTOGRAPHY	FCS_CKM.1 ensures that, if necessary, the TOE is capable of generating cryptographic keys. FCS_CKM.4 mandates the method(s) that must be satisfied when the TOE performs cryptographic key destruction. FCS_COP.1(1) requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 197 standard.
O.INTEGRITY	FMT_SMF.1 identifies the corresponding management functions. FPT_ITT.1 requires the TOE to protect the collected data and ensure its integrity when the data is transmitted to a separate part of the TOE.
O.MANAGE	The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions. FMT_MOF.1 ensures that the administrator has the ability manage the audit function. FMT_MSA.1 specifies how administrator can access security attributes. FMT_MSA.2 provides the administrator the ability to accept only secure values and modify security attributes. FMT_MSA.3 defines static attribute initialization for the WLAN information Control SFP. FMT_MTD.1 ensures that the administrator can manage audit trail data. FMT_SMF.1 identifies the management functions of TOE installation/updates and configuration/setup, and also configuration of audit trails. FMT_SMR.1 defines the specific security roles to be supported.
O.MEDIATE	FDP_IFC.1, FDP_IFF.1, FIA_UAU.1 and FIA_UID.2 ensure that the TOE has the ability to mediate packet flow based on the authentication credentials and attributes of the wireless clients.
O.RESIDUAL_ INFORMATION	FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to

	a client. FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another client's data or TSF data).
O.SELF_PROTECTION	FPT_ITT.1 ensures that the TSF protects TSF data from modification and disclosure as it is transmitted between separate parts of the TOE.
O.TOE_ACCESS	FIA_ATD.1(1)(2) Management requirements provide additional control to supplement the authentication requirements. FIA_UAU.1 ensures that administrators and clients are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable). FIA_UID.2 ensures that every admin/client is identified before the TOE performs any mediated functions. FTA_SSL.3 ensures that inactive client and administrative sessions are dropped. FTP_TRP.1 ensures that remote clients have a trusted path in order to authenticate.

Table 6: Rationale between Objectives and SFRs

6.3.2. SFR Dependencies

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them if they are included or not.

Security functional requirement	Dependency	Dependency Rationale
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	Included[2]
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.2 Restricted audit review	FAU_SAR.1 Audit review	Included

[2] FAU_GEN.2 has a dependency to FIA_UID.1 which is covered by FIA_UID.2.

Security functional requirement	Dependency	Dependency Rationale
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data	Included
FCS_CKM.1 Cryptographic key generation	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.4 Cryptographic key destruction	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Included
FCS_COP.1 Cryptographic Operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Included
FDP_IFC.1 Subset information flow control	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Included
FDP_RIP.1 Subset residual information protection	None	
FIA_ATD.1(1) Administrator attribute definition	None	
FIA_ATD.1(2) User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included[3]
FIA_UID.2 User identification before any action	None	
FMT_MOF.1 Management of security functions behavior	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included

[3] FIA_UAU.1 has a dependency to FIA_UID.1 which is covered by FIA_UID.2.

Security functional requirement	Dependency	Dependency Rationale
FMT_MSA.1 Management of security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included
FMT_MSA.2 Secure security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included[4]
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST.1 TSF testing	None	
FTA_SSL.3 TSF-initiated termination	None	
FTP_TRP.1 Trusted path	None	

Table 7: SFR's dependencies and rationale

6.3.3. SAR Rationale

The SARs specified in this ST are according to EAL2, augmented with ALC_FLR.1.

[4] FMT_SMR.1 has a dependency to FIA_UID.1 which is covered by FIA_UID.2.

7. TOE Summary Specification (ASE_TSS)

7.1. TOE Security Functions Specification

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.1 Security Functional Requirements (SFRs). Sections below covers the security audit generation mechanisms, Cryptographic support for data between the AP and the client and for both Management and data traffic, Data protection for allow or disallow certain types of traffic, Identification and authentication of users trying to connect to the network, Security management features, TSF protection, TOE access and Trusted path for remote administrators.

7.1.1. SF.Security Audit

The TOE has an audit generation mechanism to record security and non-security relevant events at a not specified level of audit.. There are several types of category for audit logs including Configuration, System, Authentication, and Client. The Configuration log/event category can include all configuration related logs. The System log category can include all system, configuration, and web server events. The Authentication log category can include all security & AAA. The Client log category can include all Clients, users, and captive portal events. Also protocol and network packet dumps are available for detailed analysis.

7.1.2. SF. Cryptographic Support

Traffic between client and Ruckus AP is encrypted using 802.11i (AES). Management traffic between Ruckus AP and Ruckus Wireless Controller is encrypted using SSH. Keys are generated using a random generator.

7.1.3. SF. User Data Protection

The TOE's policy consists of one or more rules that define the source, destination, protocol, and service type for specific traffic and whether the Wireless Controller should permit, deny, or perform other actions on the traffic that matches the rule.

7.1.4. SF. Identification and Authentication

The TOE supports role-based authentication. Wireless clients (or clients, term used interchangeably) can authenticate to an external Radius authentication server. The administrator can create an administrator account in the internal database and assign a predefined role to that account. When that user logs in to the Wireless Controller using the configured username and password, he or she is restricted based on that assigned role. In this case, the authentication mechanism is provided by the TOE and the credentials are maintained in the internal database.[5]

7.1.5. SF. Security management

The TOE provides the administrator role the capability to enable the management of security attributes, TSF data and security functions. The administrator can configure TOE security settings and policies using the Web GUI interface or the command line interface.

[5] The Wireless Controller accepts the client credentials and sends the credentials to the authentication server. The wireless clients never communicate directly with the authentication server.

7.1.6. SF. Protection of the TSF

The Wireless Controller has an internal hardware clock that provides reliable time stamps used for auditing. The internal clock is synchronized with a time signal obtained from an external NTP server. The Wireless Controller and AP run a suite of self tests during power-up which includes demonstration of the correct operation of the hardware and provide functions to verify the integrity of TSF executable code and static data. An administrator can choose to reboot the TOE to perform power-up self-test. Management traffic between Ruckus AP and Ruckus Wireless Controller is encrypted using SSH.

7.1.7. SF. TOE access

The TOE terminates a wireless client session or an administrator session after the inactivity time exceeds a configurable session idle timeout. The session idle timeout is the maximum amount of time a wireless client or an administrator may remain idle.

7.1.8. SF. Trusted path/channels

The TOE provides trusted paths for remote administrator authentication as a wired user and for wireless client authentication using a wireless connection.

For remote administrators, the TOE provides an HTTPS/SSH based trusted path from the TOE to the remote administrators for administration. SSH is also used to provide secure remote command line administration interface.

7.2. Security Functions Rationale

The table below shows the mapping between the SFRs and the implementing security functions, and a description is given in the following subsections.

Requirements / Objectives	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_SEL.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_IFC.1	FDP_IFF.1	FDP_RIP.1	FIA_ATD.1(1)	FIA_ATD.1(2)	FIA_UAU.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_ITT.1	FPT_STM.1	FPT_TST.1	FTA_SSL.3	FTP_TRP.1
SF.Security Audit	X	X	X	X	X	X																						
SF.Cryptographic Support							X	X	X																			
SF.User Data Protection										X	X	X																
SF.Identification and Authentication													X	X	X	X												
SF.Security management																	X	X	X	X	X	X	X					
SF.Protection of the TSF																								X	X	X		
SF.TOE access																											X	
SF.Trusted path/channels																												X

Table 8: Mapping SFRs to security functions

7.2.1. SF.Security Audit

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for various purposes such as security and trouble shooting. The events include startup and shutdown of audit function, and TOE security functions. At a minimum, each event includes date and time, logging level (event type), subject identity, and outcome of event.

- FAU_GEN.2: The TOE associates user id to the appropriate audit event. In other words, the user is identified by the username in the audit record.
- FAU_SAR.1: The TOE provides administrators with the capability to read all audit information from the audit records.
- FAU_SAR.2: The TOE grants read-access only to specific administrators
- FAU_SAR.3. The TOE provides the ability to apply searches, sorting, and ordering of audit data based on event type, date, and time.
- FAU_SEL.1: The TOE provides administrators the capability to include or exclude audit events based on event type.

7.2.2. SF. Cryptographic Support

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE generates 128-bit keys in compliance with FIPS PUB 197.
- FCS_CKM.4: The TOE supports a key zeroization method.
- FCS_COP.1: The TOE supports AES algorithm with a key size of 128 bits for encryption and decryption, defined by FIPS PUB 197.

7.2.3. SF. User Data Protection

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The WLAN Information Flow Policy applies to packets traffic through the network interface on the TOE. The requirement defines the subjects (wireless clients) and operation (send) covered by the scope of this requirement.
- FDP_IFF.1: The WLAN Information Flow Policy is enforced on information flows matching the WLANs defined and configured by the administrator. The policy may be configured to pass or drop traffic from clients based on WLANs and ports assigned. The client can be assigned to the WLAN configured based on authentication method.
- FDP_RIP.1: Packets read from the buffers are always the same size as those written, so no explicit zeroing or overwriting of buffers on allocation is required.

7.2.4. SF. Identification and Authentication

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1(1): The TOE's authentication mechanism uses the embedded database (the internal database) to store information about the administrators. The following information is associated with each administrator account: username and password.
- FIA_ATD.1(2): The TOE uses an external Radius server. The following information is associated with each remotely authenticated client account: client ID and client cryptographic key.
- FIA_UAU.1: The TOE will not allow the wireless client or the administrator to perform any TSF-mediated actions except identification before the authentication process completes successfully.
- FIA_UID.2: The TOE requires each wireless client or administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of that client or admin.

7.2.5. SF. Security management

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The TOE provides and restricts the capability to manage the security audit functions identified in FMT_MOF.1.

- FMT_MSA.1: The TOE provides and restricts the capability to manage the security attributes.
- FMT_MSA.2: The TOE ensures that only secure values are accepted for security attributes referenced in the FDP_IFF.1.
- FMT_MSA.3: By default, all information flow is allowed unless explicitly denied by administrator.
- FMT_MTD.1: The TOE provides and restricts the capability to manage the quering of audit events.
- FMT_SMF.1: The TOE provides interfaces to manage configuration functions.
- FMT_SMR.1: The TOE supports role-based authentication. There are two types of roles: administrator role and wireless user role.

7.2.6. SF. Protection of the TSF

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1.1: The TOE protects data from disclosure and modification when it is transmitted between separate parts of the TOE.
- FPT_STM.1: The TOE provides its own time and/or relies on an external trusted time server for this function.
- FPT_TST.1: The TOE offer a suite of self-tests to verify the correct operation of the TSF and integrity of TSF executable.

7.2.7. SF. TOE access

The TOE Access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: By default, the TOE will terminate inactive client session after a specific time interval and require clients to login again. The timeout period can be changed only by administrator. Management sessions through the WEB GUI port or the CLI port, will time out after a specific time interval.

7.2.8. SF. Trusted path/channels

The Trusted Path/Channels function is designed to satisfy the following security functional requirements:

- FTP_TRP.1: 802.1x/11i (AES) authentication will secure the network traffic to and from wireless clients at Layer 2. SSH or HTTPS are also used to provide secure remote administration interface.