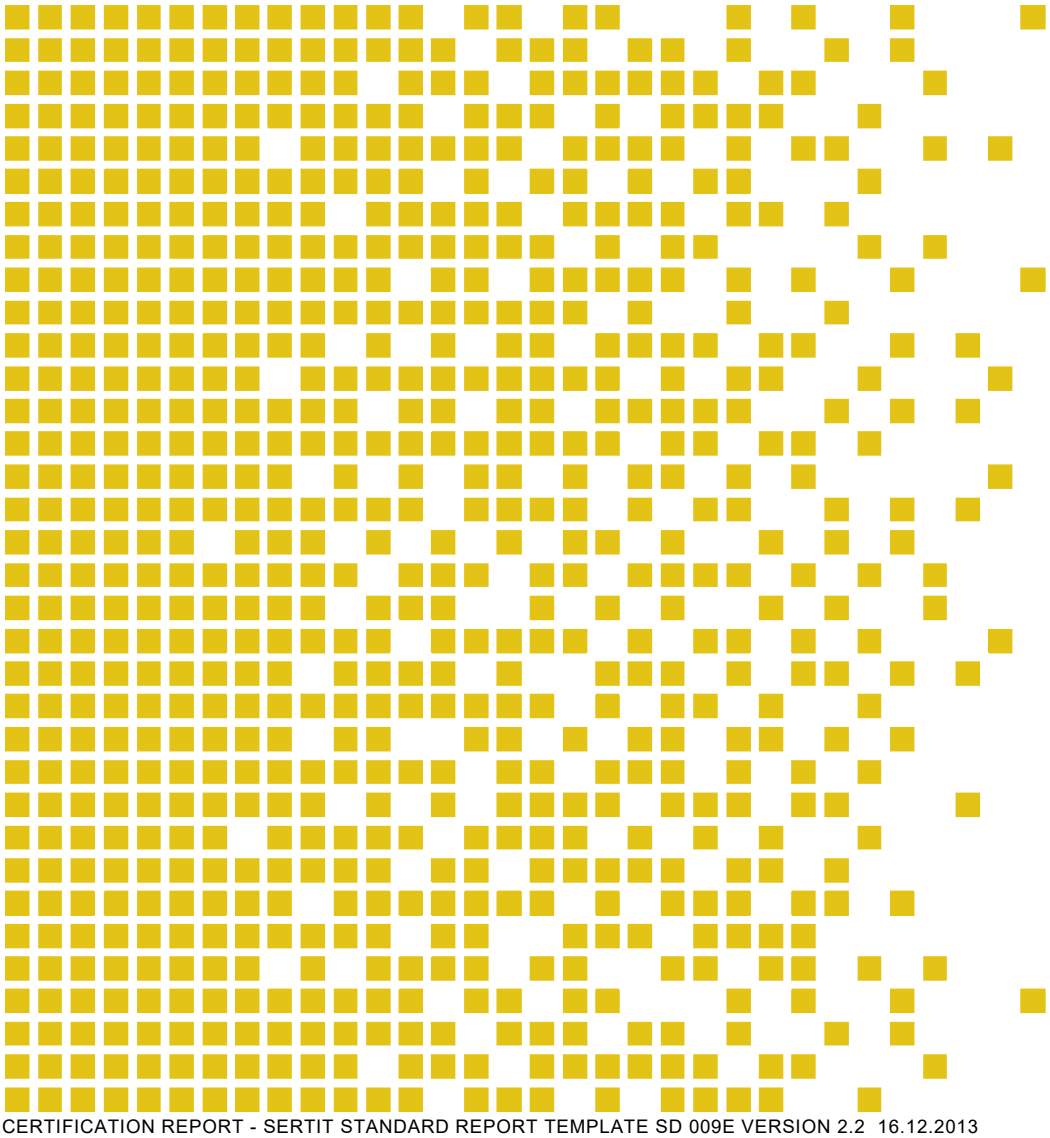
SERTIT-071 CR Certification Report

Issue 1.0 27 June 2016

Ruckus Solution



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT, which issued it, and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

Contents

Certification Statement 4

1 Abbreviations 5

2 References 6

3 Executive Summary 7
3.1 Introduction 7
3.2 Evaluated Product 7
3.3 TOE scope 7
3.4 Protection Profile Conformance 7
3.5 Assurance Level 7
3.6 Security Policies 8
3.7 Security Claims 8
3.8 Threats Countered by the TOE 8
3.9 Threats Countered by the TOE's environment 9
3.10 Threats and Attacks not Countered 9
3.11 Environmental Assumptions and Dependencies 9
3.12 Security Objectives for the TOE 9
3.13 Security Objectives for the operational environment 10
3.14 Security Functional Components 10
3.15 Evaluation Conduct 10
3.16 General Points 11

4 Evaluation Findings 11
4.1 Introduction 11
4.2 Delivery 12
4.3 Installation and Guidance Documentation 12
4.4 Misuse 12
4.5 Vulnerability Analysis 12
4.6 Developer's Tests 12
4.7 Evaluators' Tests 13

5 Evaluation Outcome 13
5.1 Certification Result 13
5.2 Recommendations 13

Annex A: Evaluated Configuration 14
TOE Identification 14
TOE Documentation 14
TOE Configuration 16

Certification Statement

Ruckus Solution (Version stated in 3.2) has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality (see Security Target chapter 5) in the specified environment when running on the platforms specified in Annex A

Author	Arne Høye Rage Certifier
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance
Approved	Kristian Bae Head of SERTIT
Date approved	27 June 2016

1 Abbreviations

AP	Access Point
CC	Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
HTTPS	Hypertext Transfer Protocol Secure
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
LAN	Local Area Network
SERTIT	Norwegian Certification Authority for IT Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WLAN	Wireless Local Area Network

2 References

[1] Ruckus Solution Security Target Version 1.8, 24.06.2016.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] ETR for the evaluation project SERTIT-071, Common Criteria EAL2 Augmented with ALC_FLR.1 Evaluation of Ruckus Solution. Version 1.1, 24 June 2016.

A complete list of the guidance documents can be found in Appendix A.

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Ruckus Solution to the developer, Ruckus Wireless, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation components.

3.2 Evaluated Product

Ruckus Solution, which 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)
- Smart Zone 100 (SZ 100)

Access Points:

- ZoneFlex R500 Smart Wi-Fi Indoor (R500)
- ZoneFlex R600 Smart Wi-Fi Indoor (R600)
- ZoneFlex T300 Smart Wi-Fi Outdoor (T300)
- ZoneFlex R710 Smart Wi-Fi Indoor (R710)
- ZoneFlex R310 Smart Wi-Fi Indoor (R310).

RuckOS 3.2.1 runs on all Wireless Controllers (SCG 200, SZ 100, vSCG).

This product is also described in this report as the Target of Evaluation (TOE). The developer was Ruckus Wireless, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

3.3 TOE scope

The Scope is described in the ST [1], chapter 1.

3.4 Protection Profile Conformance

The Security Target [1] did not claim conformance to any protection profile.

3.5 Assurance Level

The Security Target [1] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 2 augmented with

ALC_FLR.1 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [2].

3.6 Security Policies

The TOE security policies are specified in the ST [1] in chapter 3.

3.7 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional components and security functions to elaborate the objectives. The SFR's are taken from CC Part 2 [3]; use of this standard facilitates comparison with other evaluated products.

3.8 Threats Countered by the TOE

- **TT.ADMIN_ERROR** The TOE may be incorrectly configured that may result in the TOE's acquisition of ineffective security mechanisms.
- **TT.ADMIN_EXPLOIT** A person/company may gain access to an administrator account.
- **TT.CRYPTO_COMPROMISE** An attacker may compromise the cryptographic key and the data protected by the cryptographic mechanisms.
- **TT.EAVESDROPPING** Eavesdropping of the communication between clients and access points. This includes man-in-the-middle, side-channel, or other redirection attacks.
- **TT. EXPLOIT_VULN** A person/company tries to exploit vulnerability in the TOE to get unauthorized access to TOE resources.
- **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.
- **TT.MALFUNCTION** The TOE may malfunction which may compromise data or TOE resources.
- **TT.RESIDUAL_DATA** Incorrect reallocation of TOE resources.
- **TT.SPOOFING** The TOE may be subject to spoofing attack that may compromise data or TOE resources.
- **TT.TAMPERING** The TOE may be subject to physical attack that may compromise TOE resources.
- **TT. UNATTENDED_CONTROL_PLANE** The TOE may be subject to a control plane attack that may compromise TOE resources.

3.9 Threats Countered by the TOE's environment

- **TE.ADMIN_FAIL** The administrator fails to perform functions essential to the security.
- **TE.STOLEN_MOBILE_ENTITY** A stolen mobile entity with ongoing secure WLAN communication channel between client and services, through the TOE.

3.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

3.11 Environmental Assumptions and Dependencies

- **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.

3.12 Security Objectives for the TOE

- **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.

3.13 Security Objectives for the operational environment

- **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.

3.14 Security Functional Components

- 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_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1 Cryptographic operation
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes
- FDP_RIP.1 Subset residual information protection
- 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_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_ITT.1 Basic internal TSF data transfer protection
- FPT_STM.1 Reliable time stamps
- FPT_TST.1 TSF testing
- FTA_SSL.3 TSF-Initiated termination
- FTP_TRP.1 Trusted path.

3.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [5]. The Scheme is managed by the Norwegian

Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6].

SERTIT monitored the evaluation which was carried out by the evaluation facility (EVIT) Advanced Data Security. The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT in 24 June 2016. SERTIT then produced this Certification Report.

3.16 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

4 Evaluation Findings

4.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [7] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

4.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedures describe both physical and electronic software delivery.

Hardware devices are packed and sealed in factories. Each box has a security tape to identify any tampering. Distributors or customers are responsible for shipping and a service of their choice is used.

Software delivered electronically is downloaded by logging on to a support portal with username and password. The transport mechanism is secured via HTTPS session, and checksums are used to prevent tampering or masquerading of the software.

4.3 Installation and Guidance Documentation

Installation procedures and user guidance is described in detail in the supporting documents. The complete list of these documents is found in Annex A.

4.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

4.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The evaluators have searched for potential vulnerabilities and penetration tests have been devised and performed. The evaluators have not found any exploitable vulnerabilities or residual vulnerabilities in the TOE.

4.6 Developer's Tests

The evaluators have examined the developers test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests. The test plan provides information about the test configuration being used: both on the configuration of the TOE

and on any test equipment being used, as well as information about how to execute the tests.

4.7 Evaluators' Tests

The evaluators have employed a combination of a random sampling method and a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible both for the sampling of the developer's tests and for the independent testing. The number of sampled tests is 10. This is about 50% of the developer's tests. The number for independent tests is 9. The independent tests were devised to complement the developer's test.

5 Evaluation Outcome

5.1 Certification Result

After due consideration of the ETR [7], produced by the evaluators, and the conduct of the evaluation, as witnessed by the certifier, SERTIT has determined that Ruckus Solution meets the Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

5.2 Recommendations

Prospective consumers of Ruckus Solution should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 3.3 “TOE Scope” and Section 4 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE is a Wireless LAN access system (WLAN). The Wireless LAN access system defined in the ST[1] 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)
- Smart Zone 100 (SZ 100)

Access Points:

- ZoneFlex R500 Smart Wi-Fi Indoor (R500)
- ZoneFlex R600 Smart Wi-Fi Indoor (R600)
- ZoneFlex T300 Smart Wi-Fi Outdoor (T300)
- ZoneFlex R710 Smart Wi-Fi Indoor (R710)
- ZoneFlex R310 Smart Wi-Fi Indoor (R310).

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).

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.

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

TOE Documentation

The supporting guidance documents evaluated in addition to the Security Target [1] are:

A. Ruckus Guidance Documentation, v. 0.4

B. Common Criteria Guidance Supplement document, v. 2
C. SmartZone 3.2.1 Patch 1Release Notes, April 2016
D. R600 Access Point Quick Setup Guide, September 2016
E. R710 Access Point Quick Setup Guide, April 2015
F. Ruckus Wireless™ SmartCell Gateway™ 200 Charging Interface Reference Guide for SmartZone 3.2.1, January 2016
G. Ruckus Wireless™ SmartCell Gateway™ 200 Getting Started Guide for SmartZone 3.2.1, January 2016
H. Ruckus Wireless™ SmartCell Gateway™ 200 Gn Interface Reference Guide for SmartZone 3.2.1, January 2016
I. Ruckus Wireless™ SmartCell Gateway™ 200 HLR Interface Reference Guide for SmartZone 3.2.1, January 2016
J. Ruckus Wireless™ SmartCell Gateway™ 200 S2a Interface Reference Guide for SmartZone 3.2.1, January 2016
K. Ruckus Wireless™ SmartCell Gateway™ 200 Standard Compliance Report for SmartZone 3.2.1, January 2016
L. Ruckus Wireless™ SmartCell Gateway™ 200 Tunneling Interface Reference Guide for SmartZone 3.2.1, January 2016
M. Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High-Scale AAA (RADIUS) Interface Reference Guide for SmartZone 3.2.1, April 2016
N. SmartCell Gateway™200/Virtual SmartZone™ High-Scale Administrator Guide for Release 3.2.1, 20160215(1)
O. Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone™ High Scale Alarm and Event Reference Guide for SmartZone 3.2.1, April 2016
P. Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High-Scale Command Line Interface Reference Guide for SmartZone 3.2.1, May 2016
Q. Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High-Scale Hotspot 2.0 Reference Guide for SmartZone 3.2.1, January 2016
R. Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone™ High Scale SNMP MIB Reference Guide for SmartZone 3.2.1, April 2016
S. Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High Scale Hotspot WISPr Reference Guide for SmartZone 3.2.1, January 2016
T. Ruckus Wireless™ SmartZone™ 100 Getting Started Guide for SmartZone 3.2.1, January 2016
U. Ruckus Wireless™ SmartZone™ 100 Quick Setup Guide for SmartZone 3.2.1, January 2016
V. Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone Essentials AAA (RADIUS) Interface Reference Guide for SmartZone 3.2.1, January 2016

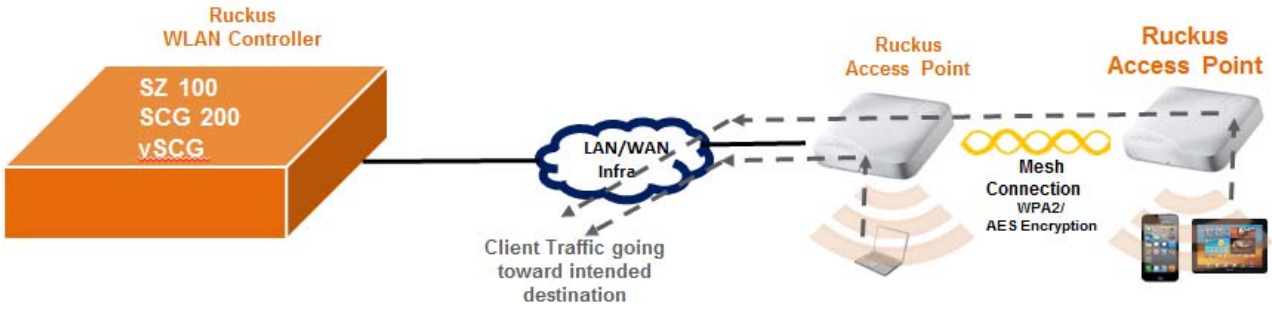
W. SmartZone™ 100/Virtual SmartZone™ Essentials Administrator Guide for Release 3.2.1, 20160203(1)
X. Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone™ Essentials Alarm and Event Reference Guide for SmartZone 3.2.1, April 2016
Y. Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone Essentials Command Line Interface Reference Guide for SmartZone 3.2.1, May 2016
Z. Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone Essentials Hotspot 2.0 Reference Guide for SmartZone 3.2.1, January 2016
AA. Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone Essentials Hotspot WISPr Reference Guide for SmartZone 3.2.1, January 2016
BB. Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone™ Essentials SNMP MIB Reference Guide for SmartZone 3.2.1, April 2016
CC. Ruckus Wireless™ Virtual SmartZone™ Getting Started Guide for SmartZone 3.2.1, January 2016
DD. Ruckus Wireless™ Virtual SmartZone™ Quick Setup Guide for SmartZone 3.2.1, January 2016
EE. ZoneFlex-T300- Mounting Guide -2014/09/04
FF. AP tunnelmgr and R-GRE module document
GG. Ruckus Wireless™ SmartCell Gateway™ 2.0 SCG–AAA Interface Control Reference Guide, April 2012
HH. Export-SCG-AP-Statistics document
II. Ruckus Wireless™ SmartZone™ 200 and Virtualized SmartZone Essentials Command Line Interface Reference Guide for SmartZone 3.2.1, January 2016
JJ. SSG 200 3.2.1.0.93 CLI Command Document
KK. Functional Specification for Communication Protocol for Wireless Service Gateway (WSG) SharePoint, Version 2.29
LL. ZoneFlexTM Access Point Simple Network Management Protocol Release 9.8 Reference Guide, June 2014
MM. Virtual SmartZone (High Scale) Public API Reference Guide, http://docs.ruckuswireless.com/vscg-carrier/vsz-h-public-api-reference-guide-3-2-1.html

TOE Configuration

The following configurations were used for testing:

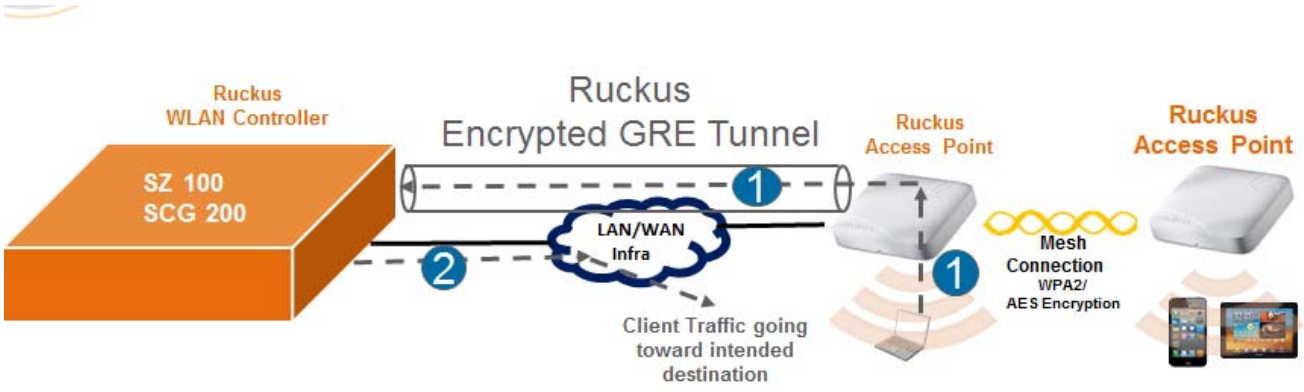
Ruckus Wireless Controllers and Ruckus Smart Wi-Fi Aps are deployed in two different models; distributed deployment model for SCG 200, SZ-100 and vSCG, and centralized deployment model for SCG 200 and SZ-100.

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



Distributed 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.



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.

Evaluated configuration:

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

Not covered as part of the evaluated configuration:

- 3rd Party APs
- 3rd Party Soft-GRE Concentrator
- External Syslog, NTP, SNMP servers
- Built-in Captive Portals
- GTP Tunnel