Virtual SmartZone (vSZ) WLAN Controller

Version 5.1.1.3

FIPS 140-2 Level 1 Non-Proprietary Security Policy

By Ruckus Wireless, Inc.

Document Version Number: 1.3

Table of Contents

1. Module Overview

Ruckus Networks Virtual SmartZone (vSZ)

Ruckus VirtualSmart Zone (vSZ), is a Network Functions Virtualization (NFV) based WLAN Controller for customers who desire a carrier-class solution that runs in the cloud. It supports all the WLAN Controller features of the industry leading physical controllers, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services. The vSZ is a software module, which is defined as a multi-chip standalone cryptographic module by FIPS 140-2.

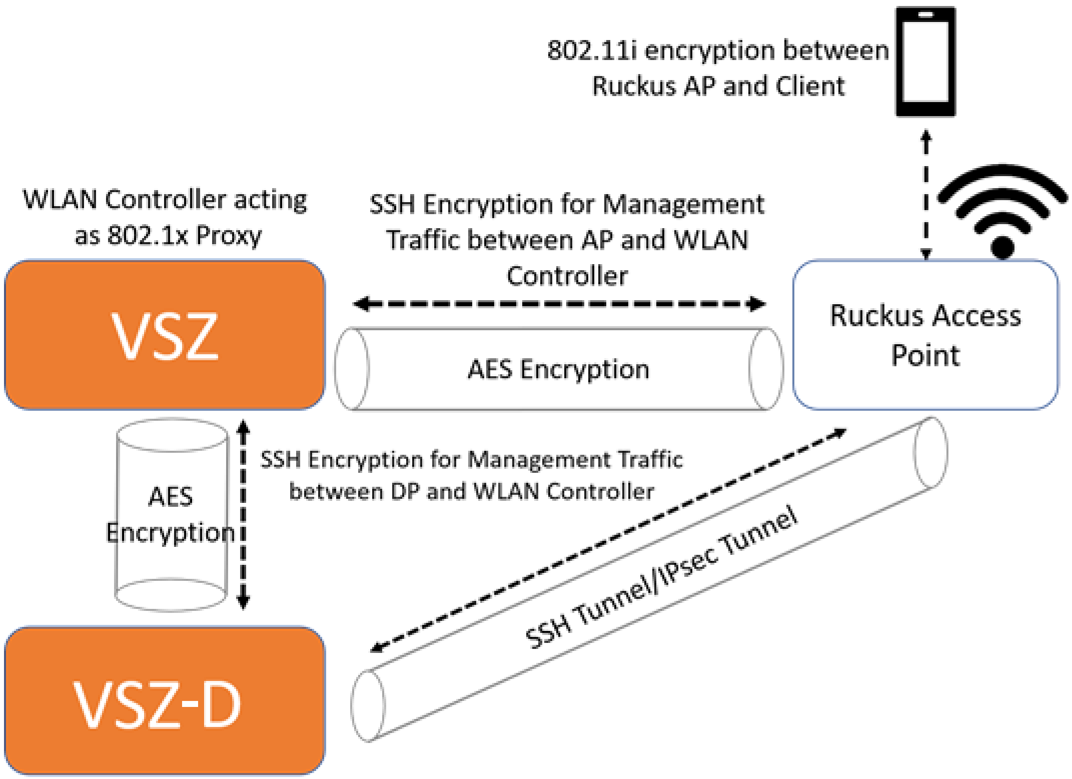
802.11i encryption between
Ruckus AP and Client
WLAN Controller acting
as 802.1x Proxy
SSH Encryption for Management
Traffic between AP and WLAN
Controller
VSZ
AES Encryption
Ruckus Access
Point
AES
Encryption
SSH Encryption for Management Traffic
between DP and WLAN Controller
SSH Tunnel/IPsec Tunnel
VSZ-D

Figure 1: Encryption Between AP and Controller[1]

FIPS 140-2 conformance testing was performed at Security Level 1. The following configurations were tested by the lab.

Table 1: Tested Configuration

Module	GPC & Processor	Operating System
Ruckus Networks Virtual SmartZone (vSZ) SW Version: 5.1.1.3	Dell PowerEdge R740; Intel(R) Xeon(R) CPU Platinum 8160 @ 2.10GHz with AES-NI; & without AES-NI	CentOS 6.8 on VMware ESXi 6.5.0

[1] In Figure 1, AP refers to Ruckus Access Point and DP refers to the vSZ-D module, where DP is an abbreviation of Data Plane.

The Cryptographic Module meets FIPS 140-2 Level 1 requirements.

Table 2: Module Security Level Statement

FIPS Security Area	**Security Level**
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

The cryptographic boundary of the module is shown below.

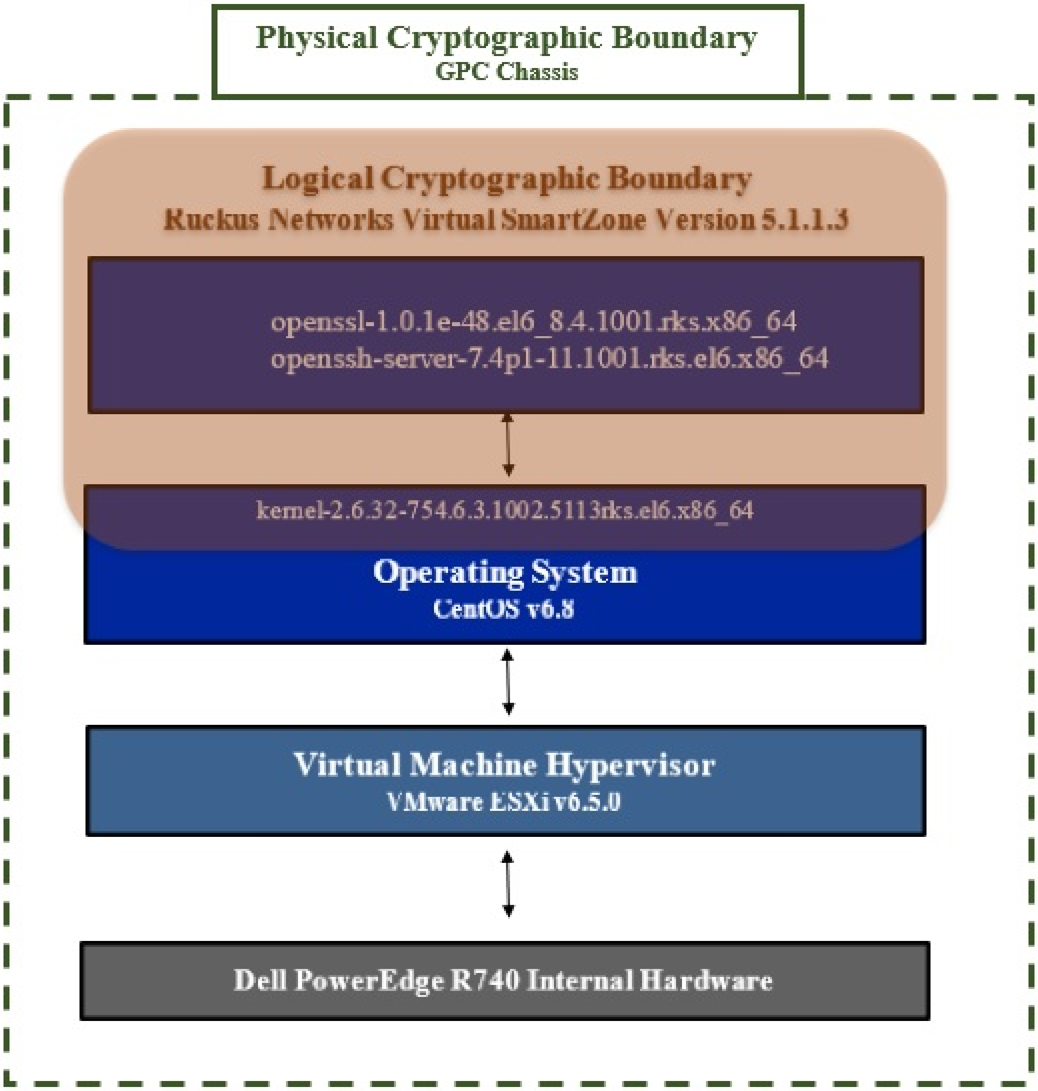
Physical Cryptographic Boundary
GPC Chassis
Logical Cryptographic Boundary
Ruckus Networks Virtual SmartZone Version 5.1.1.3
openssl-1.0.1e-48.el6_8.4.1001.rks.x86_64
openssh-server-7.4p1-11.1001.rks.el6.x86_64
kernel-2.6.32-754.6.3.1002.5113rks.el6.x86_64
Operating System
CentOS v6.8
Virtual Machine Hypervisor
VMware ESXi v6.5.0
Dell PowerEdge R740 Internal Hardware

Figure 2: Block Diagram for Ruckus Networks Virtual SmartZone (vSZ)

The Ruckus Virtual SmartZone(vSZ) logical cryptographic boundary includes shared object and the binary of OpenSSL, the binary of OpenSSH and the AES-NI module of the Kernel. The version list of the cryptographic components within the vSZ module is listed below:

- openssl-1.0.1e-48.el6_8.4.1001.rks.x86_64
- openssh-server-7.4p1-11.1001.rks.el6.x86_64
- kernel-2.6.32-754.6.3.1002.5113rks.el6.x86_64

2. Modes of Operation

The module is intended to always operate in the FIPS Approved mode. A provision is made to disable/enable FIPS mode via configuration (Login CLI -> enabled mode -> fips enable/disable). In addition to running the `fips enable` command, an operator must follow the procedural rules specified in Section 8 to remain in the Approved mode. Refer to the Ruckus FIPS Configuration Guide for more information.

2.1 Approved and Allowed Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation. Note that in some cases, more algorithms/ modes of operation have been tested than are utilized by the Module. Implementations in **black** text are used, **gray** text shows tested but not used configurations in the table below.

Table 3: Approved Cryptographic Functions[4]

CAVP Cert #	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
Linux Kernel					
C814	AES	FIPS 197, SP 800-38A	CBC	128, 192, 256	Data Encryption/ Decryption
C814	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160, 192, 256, 320, 384, 448, 512	Message Authentication
C814	SHA	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest

CAVP Cert #	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
OpenSSL/ OpenSSH					
5098	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, CFB1, CFB8, CFB128, CTR, ECB, GCM[1], OFB	128, 192, 256	Data Encryption/ Decryption
(vendor affirmed)	CKG	SP 800-133	Section 6.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation[3]
			Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		
			Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
C815	CVL	SP 800-135	SNMPv3	See Table 6 for protocol information.	Key Derivation[2]
		SP 800-135	TLSv 1.2, SSH	SHA-1 / 224 / 256 / 384 / 512 SHA-256 / 384 / 512 See Table 6 for protocol information.	Key Derivation[2]
		SP 800-135	IKEv2	See Table 6 for protocol information.	Key Derivation[2]
		SP 800-56A rev1	ECC CDH	- B-233/283/409/571 - K-233/283/409/571 - P-224/256/384/521 * P-224 is only used to meet power-up self-test requirements	Key Agreement

CAVP Cert #	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
		SP 800-135	RSADP		Key Derivation[2]
1904	DRBG	SP 800-90A	Counter, Hash, HMAC	Counter:128, 192, 256 Hash: SHA-1, 224, 256, 384, 512 HMAC: SHA-1, 224, 256, 384, 512	Deterministic Random Bit Generation
C815	DSA	FIPS 186-4	Key Generation	L=2048, N=224, 256 L=3072, N=256	Diffie-Hellman Key Generation
1323	ECDSA	FIPS 186-4		Key Generation: - B-233/283/409/571 - K-233/283/409/571 - P-224/256/384/521 Signature Generation: - P-256* w/SHA-224/256/384/512 - P-384 w/ SHA-224/256/384/512 - P-224/521, K-233/283/409/571, B-233/283/409/571 w/SHA-224/256/384/512 * P-256 signature generation is only used for power-up self-tests Signature Verification: P-192/224/256/384/521, B-163/233/283/409/571, K-163/233/283/409/571 w/ SHA-1/224/256/384/512 (operator defined)	Key Generation, Digital Signature Generation and Verification

CAVP Cert #	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
				Approved per IG A.14: any non-testable ECDSA curve generated in compliance with Section 6.1.1 of FIPS 186-4 and providing at least 112 bits of strength.	
3400	HMAC	FIPS 198-1	HMAC-SHA1 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	80, 96, 128, 160 112,128,160,192,224 128, 192, 256 192, 256, 320, 384 256, 320, 384,448, 512	Message Authentication
5098, 3400	KTS	SP 800-38F	AES with HMAC SHA-1/256/384/512	AES: 128, 192, 256 HMAC: 160, 256, 384, 512	Authenticated Encryption, Authenticated Decryption
5098	KTS	SP 800-38F	AES-GCM	AES: 128, 192, 256 Key establishment method provides 128 or 256 bits of encryption strength	Authenticated Encryption, Authenticated Decryption
2760	RSA	FIPS 186-2 FIPS 186-4	ANSI X9.31 PKCSPSS PKCS1 v1.5	Key Generation: (186-2 and 186-4) - 2048, 3072, 4096-bit Signature Generation: (186-4) - 2048*/3072-bit w/ SHA-224, 256, 384, 512	Key Generation Digital Signature Generation and Verification

CAVP Cert #	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
				* RSA-2048 signature generation is only used for power-up self-tests <u>Signature Verification:</u> (186-2 and 186-4) -1024/1536/2048/ 3072/4096-bit w/ SHA-1/224/256/384 /512 (operator defined) Approved per IG A.14: any non-testable RSA modulus greater than 2048 bits. 4096-bit SigVer tested under 186-2.	
4146	SHA	FIPS 180-4	SHA1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest

[1] AES GCM IV IG A.5 Compliance:

- SSH: The IV is only used in the context of the AES GCM mode encryptions within the SSHv2 protocol. The module is compliant with RFCs 4252, 4253 and RFC 5647. The AES GCM IV satisfies the following conditions:
  - If the invocation counter reaches its maximum value 2^64 – 1, the next AES GCM encryption is performed with the invocation counter set to 0.
  - No more than 2^64 – 1 AES GCM encryptions may be performed in the same session. The SSH session is reset for both the client/server after one GB of data (2^23 block encryptions) or one hour whichever comes first.
  - When a session is terminated for any reason, a new key and a new initial IV are derived.
- TLS: The module is compatible with TLSv1.2 and the module supports acceptable GCM ciphersuites from SP 800-52 Rev 1, Section 3.3.1. The ciphersuites are listed in Table 6. The 64-bit nonce of the IV is deterministic. It will take 2^64 increments for the IV invocation field to wrap. The module does not enter an error state if wrapping occurs because it is inconceivable that this value can wrap around. Assuming a time of 1ns per generation operation (several orders of magnitude faster than currently possible) it would take over 584 years to wrap around.

[2] No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[3] The module directly uses the output of the DRBG.

[4] The module implements only the modes, data size, and key sizes in the Approved algorithm table or modes that were tested but not implemented. Gray text indicates which moduli, sizes, or modes may be tested but not implemented.

2.2 Non-FIPS Approved but Allowed Cryptographic Functions

The following non-FIPS Approved but allowed cryptographic algorithms are used in FIPS approved mode of operation.

Table 4: Non-FIPS Approved but Allowed Cryptographic Functions

Algorithm	Caveat	Use
Diffie Hellman (CVL Cert. #C815) – TLS v1.2	Provides between 112 and 128 bits of encryption strength	Used during TLS handshake
EC Diffie Hellman (CVL Cert. #C815 with CVL Cert. #C815) – IKEv2	Provides 192 bits of encryption strength	Used during SSH, IKEv2/ IPsec and TLS handshake. See Table 6 for curve sizes used in each protocol.
EC Diffie Hellman (CVL Cert. #C815 with CVL Cert. #C815) - SSH	Provides 192 bits of encryption strength	
EC Diffie Hellman (CVL Cert. #C815 with CVL Cert. #C815) - TLS v1.2	Provides between 128 and 256 bits of encryption strength	
HMAC-MD5	No security claimed per IG 1.23	Used in RADsec
NDRNG	The module generates cryptographic keys whose strength is modified by available entropy. The vSZ provides 128 bits of security.	Used to seed the SP 800-90A DRBG. (Provides a 256-bit seed)

2.3 Non-FIPS Approved Cryptographic Functions

The following non-FIPS approved cryptographic algorithms are used only in the non-Approved mode of operation.

Table 5: Algorithms/Protocols Available in Non-Approved Mode

Algorithm	Use
chacha20-poly1305@openssh.com, umac-64@openssh.com,hmac-ripemd160,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com DSA, ED25519	OpenSSH
EAP-Cisco, EAP-SIM, EAP-AKA, EAP-MSCHAP-V2, EAP-AKA’, MD5-Challenge	Radius
MD5, DES	SNMP
MD5, DES Triple-DES (non-compliant)*	OpenSSL
AES CBC (non-compliant)* TLSv1.2 Key Derivation (non-compliant)* RSASP (non-compliant)* DRBG (non-compliant)* HMAC (non-compliant)* RSA PKCS1 v1.5 (non-compliant)* SHS (non-compliant)*	OpenJDK AAA Test Suite

*Triple-DES and OpenJDK library are non-compliant. OpenJDK algorithm power-up tests are performed but are not used except for testing communication with external AAA server. Using the OpenJDK AAA Test Suite constitutes exiting the FIPS Approved Mode, as stated in Section 8.

2.4 Protocols Used in the FIPS Approved Mode of Operation

Table 6: Protocols Available in the Approved Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
IKEv2 [IG D.8 and SP 800-135]	Oakley 20 (P-384)	RSA 3072 Pre-shared secret ECDSA P-384	AES CBC 128/192/256	HMAC-SHA-1 HMAC-SHA-2-256 HMAC-SHA-2-384 HMAC-SHA-2-512
IPsec ESP	Oakley 20 (P-384)	IKEv2	AES-CBC-128/192/256	HMAC-SHA-1 HMAC-SHA-2-256 HMAC-SHA-2-384 HMAC-SHA-2-512
SSHv2 [IG D.8 and SP 800-135]	ECDH-sha2-nistp256, ECDH-sha2-nistp384, ECDH-sha2-nistp521	ECDSA P-384 RSA 3072	AES-CTR-128/256 AES256-GCM@openssh.com	HMAC-SHA-1-96, HMAC-SHA-2-256, HMAC-SHA-2-512
TLS [IG D.8 and SP 800-135]	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384			TLS v1.2
	Ephemeral ECDH	RSA	AES-GCM-256	HMAC-SHA-384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	Ephemeral ECDH	RSA	AES-GCM-128	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256			TLS v1.2
	Ephemeral ECDH	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384			TLS v1.2
	Ephemeral ECDH	RSA	AES-CBC-256	HMAC-SHA-384
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256			TLS v1.2
	Ephemeral DH	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256			TLS v1.2
	Ephemeral DH	RSA	AES-CBC-256	HMAC-SHA-256
SNMPv3	N/A	N/A	AES-CFB-128	HMAC-SHA1

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
NTP	N/A	SHA-1	N/A	N/A
RADIUS (only used within RADsec)	N/A	HMAC-MD5	N/A	N/A
EAP	N/A	PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-TLS EAP-TTLS	N/A	N/A

2.5 Approved Certificate Sizes

Crypto Officer is able to upload certificates and only the approved certificate sizes can be loaded into the module in the approved mode.

3. Ports and Interfaces

The following table describes logical interfaces of the module.

Table 7: FIPS 140-2 Logical Interfaces

Logical Interface	Description
Data Input	Input parameters that are supplied to the API commands
Data Output	Output parameters that are returned by the API commands
Control Input	API commands
Status Output	Return status provided by API commands

4. Roles and Services

The module supports a Crypto Officer role, User Role, and AP (Access Point) Role. The Crypto Officer installs and administers the module. The Users and APs use the cryptographic services provided by the module. The module provides the services shown below in Table 8.

Table 8: Approved Mode Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write Z – Zeroize
Reboot/ Self-test	Crypto Officer User	All (not including instances in NVM): Z
Zeroization	Crypto Officer	All: Z
[1]Software update	Crypto Officer	Software update key: R
Show status	Crypto Officer User AP	N/A
Login	Crypto Officer User	Password: R SSH Keys: R, W, E TLS Keys: R, W, E DRBG seed: R
SSH Tunnel	Crypto Officer User AP	Password: R, W, E SSH Keys: R, W, E DRBG seed: R
Configuration	Crypto Officer	Password: R, W, E SSH Keys: R, W, E TLS Keys: R, W, E DRBG seed: R
RadSec	AP	TLS Keys: R, W, E DRBG seed: R, W, E Radius Secret: R
NTP	Crypto Officer	NTP Keys: R, W, E
HTTPS/TLS	Crypto Officer User AP	TLS Keys: R, W, E DRBG seed: R
IPsec tunnel	Crypto Officer AP	IKE Keys: R, W, E
EAP authenticator (EAP-TLS, EAP-TTLS, EAP-PEAP)	AP	SSH Keys: R, W, E DRBG seed: R, W, E TLS Keys: R, W, E
SNMPv3	Crypto Officer User	Password: E SNMP Keys: R, W, E
FIPS mode enable/disable	Crypto Officer	N/A

[1]*Invoking the Software Update service will result in a version of the product that is out of scope of this validation and therefore not validated. To remain in the validated configuration the Software Update service shall not be invoked*

Table 9: Non-Approved Mode Roles and Services

Service	Corresponding Roles
Self-test	Crypto Officer User
Reboot	Crypto Officer User
Zeroization	Crypto Officer
Software update	Crypto Officer
Show status	Crypto Officer User AP
Login	Crypto Officer User
SSH Tunnel	Crypto Officer User AP
Configuration	Crypto Officer
HTTPS/TLS	Crypto Officer User AP
IPsec tunnel	AP
AAA Test	Crypto Officer
EAP authenticator _(EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA)	AP
SNMPv2	Crypto Officer User
SNMPv3	Crypto Officer User
FIPS mode enable/disable	Crypto Officer
Diagnostics	N/A: intended for manufacturing only; the module requires authorization by the admin before accessing

The module supports the following authentication mechanisms:

Table 10: Authentication Mechanisms

Role	Authentication Type	Authentication Mechanisms	Authentication Strength
User Role (Monitoring user)	Role-based (default UID is used)	User ID and Password Minimum length of 8 characters comprised the following available characters: 26 lowercase 26 uppercase 10 numeric 10 special	The authentication strength is 1/72^8 which means the probability of a random attempt or a false acceptance will succeed is less than 1 in 1,000,000 An operator is able to configure a try limit within the range of 1-100, therefore the maximum attempts to authenticate in a one-minute period is limited to 100 in the Approved mode of operation. For multiple attempts over a 1-minute period, probability of a random attempt or a false acceptance will succeed is 100/(72^8) which is less than 1 in 100,000.
CO Role (Configuration user)	Role-based (admin ID is non-modifiable)	Admin ID and Password Minimum length of 8 characters comprised the following available characters: 26 lowercase 26 uppercase 10 numeric 10 special	The authentication strength is 1/72^8 which means the probability of a random attempt or a false acceptance will succeed is less than 1 in 1,000,000 An operator is able to configure a try limit within the range of 1-100, therefore the maximum attempts to authenticate in a one-minute period is limited to 100 in the Approved mode of operation. For multiple attempts over a 1-minute period, probability of a random attempt or a false acceptance will succeed is 100/(72^8) which is less than 1 in 100,000.
AP Role (Access Point User)	Identity-based	SSH RSA key (3072 bits)	The authentication strength of RSA-3072 with SHA-384 verification is 1/2^128 which means the probability of a random attempt or a false acceptance will succeed is less than 1 in 1,000,000 The module is incapable of processing more than approximately 1,000 RSA signature verifications per minute, therefore the probability of randomly successfully authenticating is 1000/(2^128) which is less than 1 in 100,000 over a 1-minute period.

5. Operational Environment

The operating system is restricted to a single operator mode of operation in a modifiable operational environment, wherein concurrent operators are explicitly excluded.

This software cryptographic module is implemented in client/server architecture and is intended to be used on both the client and the server. It will be used to provide cryptographic functions to the client and server applications. Since this module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the module, even when the server application is serving multiple clients.

Ruckus affirms that the following platform is equivalent to the tested and validated platform listed in Table 1, and that the module will function in the same way and provide the same security services:

Processor: Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI
Operating System: CentOS 6.8 on KVM on Ubuntu 16.04.2 LTS

6. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 11: Cryptographic Keys and CSPs

Key	Description/Usage
TLS Master Secret	Used to derive TLS Encryption Key and TLS Authentication Key
TLS Pre-Master Secret	Used to derive TLS Master Secret
TLS Encryption Key	AES key used during encryption and decryption of data within the TLS protocol
TLS Authentication Key	HMAC key used to protect integrity of data within the TLS protocol

TLS Server RSA Private Key	Used during the TLS handshake to sign the server certificate
TLS Server RSA Public Key	Used during the TLS handshake to authenticate to the TLS client
TLS Client RSA Public Key	Used during the TLS handshake to authenticate the TLS client
TLS DH/ ECDH Host Private Key	DH or ECDH private key used to establish the TLS Pre-Master Secret
TLS DH/ ECDH Host Public Key	DH or ECDH public key sent to the TLS client to establish the TLS Pre-Master Secret
TLS DH/ ECDH Client Public Key	DH or ECDH public key used to establish the TLS Pre-Master Secret
DRBG Entropy Input	Entropy Input for the SP800-90A CTR DRBG
DRBG Internal State	Internal state of the SP 800-90A CTR DRBG (Key and V)
User Password	Password used to authenticate the User (at least 8 characters)
Enable Password	Password used by the Crypto Officer to enable the CLI (at least 8 characters)
Crypto Officer Password	Password used to authenticate the Crypto Officer (at least 8 characters)
SSHv2 RSA/ ECDSA Private Key	RSA or ECDSA private key used during the SSH handshake to sign the host or client certificate, depending on whether the module is acting as the SSH client or host
SSHv2 Host RSA/ ECDSA Public Key	RSA or ECDSA public key used during the SSH handshake to authenticate the SSH host
SSHv2 Client RSA/ ECDSA Public Key	RSA or ECDSA public key used during the SSH handshake to authenticate the SSH client
SSHv2 ECDH Private Key	ECDH private key used to derive SSH Session and Authentication Keys
SSHv2 Host ECDH Public Key	ECDH public key sent to the TLS client to derive SSH Session and Authentication Keys
SSHv2 Client ECDH Public Key	ECDH public key used to derive SSH Session and Authentication Keys
SSHv2 Session Key	AES encryption key used to secure an SSH session

SSHv2 Authentication Key	HMAC key used to authenticate and integrity-check an SSH session
IKEv2/ IPsec Encryption Key	AES Key used to encrypt session data
IKEv2/ IPsec Authentication Key	HMAC Key used to authenticate and integrity-check a session
IKEv2/ IPsec ECDH Private Key	ECDH private key used to derive IKE/ IPsec Session and Authentication Keys
IKEv2/ IPsec Host ECDH Public Key	ECDH public key sent to the IKE/ IPsec client to derive IKE/ IPsec Session and Authentication Keys
IKEv2/ IPsec Client ECDH Public Key	ECDH public key used to derive IKE/ IPsec Session and Authentication Keys
IKEv2/ IPsec RSA/ ECDSA Private Key	RSA or ECDSA private key used during the IKE/ IPsec handshake to sign the host certificate
IKEv2/ IPsec Host RSA/ ECDSA Public Key	RSA or ECDSA public key used during the IKE/ IPsec handshake to authenticate to the SSH client
IKEv2/ IPsec Client RSA/ ECDSA Public Key	RSA or ECDSA public key used during the IKE/ IPsec handshake to authenticate the SSH client
IKEv2/ IPsec Pre-Shared Key	Used to authenticate IKE/ IPsec peers to each other
Software Upgrade Key	Used to verify the signature of software being loaded into the module
SNMP Passphrases	Separate passphrases used to derive the SNMPv3 auth key and SNMPv3 privacy key respectively (8-63 characters)
SNMP Authentication Key	Used to authenticate SNMPv3 packet using HMAC-SHA-1
SNMP Privacy Key	Used to encrypt SNMPv3 packet using AES-CFB-128
RADIUS Secret	Used to authenticate with the RadSec server (at least eight (8) characters)
NTP Key	Used to authenticate with the NTP server (40 characters in approved mode, no restriction in non-Approved mode)

7. Self-Tests

The module performs the following power-up and conditional self-tests. Running power up self-tests does not involve action from the operator. Upon failure or a power-up or conditional self-test the module halts its operation and enters a quarantine state. The following table describes each self-test implemented by the module.

Table 12: Power-Up Self-Tests

Algorithm	Test
Linux Kernel	
AES	AES-128/ 192/ 256 CBC KAT (encryption/ decryption)
HMAC	HMAC SHA-256 KAT
SHA	SHA-1/ 256/ 384/ 512 KAT
OpenSSL/ OpenSSH	
AES	AES-128 CBC KAT (encryption/decryption)
SHS	SHA-1/ 256/ 512 KAT
HMAC	HMAC SHA-1/ 256/ 384/ 512 KAT
SP800-90A DRBG	AES-256 CTR DRBG KAT (DRBG health tests per SP 800-90A Section 11.3)
DSA	(L=2048, N=256) with SHA-384 KAT (signature generation/ verification)
RSA	RSA-2048 w/SHA-384 KAT (signature generation/ verification)
ECDH	P-256 KAT (includes Primitive “Z” computation)
ECDSA	P-256 KAT (signature generation/ verification)
Software integrity	RSA-4096 with SHA384 signature verification during boot-up

Table 13: Conditional Self-Tests

Algorithm	Test
SP800-90A DRBG	Continuous Random Number Generator test
NDRNG	Continuous Random Number Generator test
RSA	Pairwise Consistency Test

ECDSA	Pairwise Consistency Test
Software Load	RSA-4096 with SHA-384 with signature verification

8. Installation, Configuration, and Secure Operation

8.1 Module Initialization

The following steps shall be executed by the Cryptographic Operator for the module to operate in the validated FIPS configuration. For additional help with system requirements, refer to the Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and APs:

- vSZ Installation and Configuration with FIPS Image:
  - Create and register the Virtual Machine on VMware ESXi and deploy the VM.
  - Power on the module and open a console window to log in to the vSZ CLI.
  - At the login prompt, login with the administrator username and password
  - Type the enable (en) command and the admin password to change to Privileged EXEC mode.
  - Type "fips enable" command and hit enter
  - Enter "yes" at the prompt and the module will continue setup and reboot
  - After reboot, login with the default credentials
  - Enter the "en" command for EXEC mode
  - Enter "setup" command and hit enter
  - At the FIPS Setting prompt, select option 2 to keep the current FIPS mode
  - At the vSZ profile prompt, select option 2 to select the High Scale vSZ profile
  - Type "y" at the "are you sure" confirmation prompt and hit enter
  - The next series of prompts will take the operator through the IP Version Support settings. Answer the series prompts appropriately for the network. Prompts include **address type**; **IP configuration**; and **DNS Server Settings**
  - Type "y" and hit enter when prompted to apply the settings
  - Type "y" and hit enter to accept the settings
  - Type the "setup" command and hit enter
  - When prompted to setup network, type "n" and hit enter

  - Opt to create or join cluster as appropriate and answer the following prompts appropriately for the cluster. Prompts include: **Cluster name, controller description, domain name**
  - Type "y" and hit enter at the verification prompt
  - Enter the controller name and hit enter
  - Answer appropriately when prompted for NAT
  - Enter system time, system date, system time zone

  - Enter "y" when asked "Convert ZoneDirector Aps in factory settings to vSZ Aps automatically (y/n)

- Enter new admin password when prompted
- Enter the CLI enable command password
- The module will complete the setup and reboot
- Upon reboot the operator will login with the newly configured password
- FIPS status can be verified by using the “fips status ?” command. If FIPS is enabled the command will return “FIPS compliance is Enable”

8.2 Procedural Rules

The following procedural rules shall be executed and maintained by the Cryptographic Officer for the module to operate in the approved mode of operation. Failure to adhere to any of the following rules will result in the module operating in a non-approved mode of operation.

- An operator shall zeroize all keys/ CSPs when switching between the Approved and non-Approved mode (or vice versa).
- Approved key sizes are used by default, however the operator is capable of loading their own TLS certificates containing non-Approved RSA key lengths. Only Approved RSA key lengths specified in Table 3 shall be used.
- An operator shall not attempt to access the module’s BIOS. In particular, an operator shall not change the port configurations specified in Section 3 of this Security Policy.
- The module does not enforce a limit on the number of authentication attempts without first being configured to do so. The User and Cryptographic Officer shall have an authentication try limit configured between the range of 1-100.
- An operator shall not evoke the OpenJDK AAA Test Service as use of these algorithms constitutes exiting the Approved mode of operation.
- The Software Update Service shall not be evoked. Updating the software will result in a version of the product that is out of scope and therefore not validated.

9. References

Table 14: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)

Reference	Specification
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions