Huawei R250, R230, and R240
Remote Radio Units

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 0.6
Date: August 8, 2017

Contents

Tables

Figures

References and Definitions

Ref	Full Specification Name
ESP	Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, Internet Engineering Task Force, December 2005.
ESP-B	Law, L. and J. Solinas, "Suite B Cryptography Suites for IPsec", RFC 6379, Internet Engineering Task Force, October 2011.
LDAP	Semersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, Internet Engineering Task Force, June 2006.
RADIUS	Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS), RFC 2865, Internet Engineering Task Force, June 2000.
SSH	Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Connection Protocol", RFC 4254, Internet Engineering Task Force, January 2006.
SSH-B	K. Igoe, "Suite B Cryptography in Suites for Secure Shell (SSH)", Internet Engineering Task Force, May 2011.
TLS	Dierks, T., and E. Rescoria, "The Transport Layer Security (TLS) Protocol Version 1.2". RFC 5246, Internet Engineering Task Force, August 2008.
TLS-B	Salter, M and R. Housely, "Suite B Profile for Transport Layer Security (TLS)", Internet Engineering Task Force, January 2012.

Table 1 – References

Term	Definition
AAA	Authentication, Authorization and Accounting - access control, policy enforcement and auditing framework for computing systems, e.g. LDAP
ACL	Access Control List
ARP	Address Resolution Protocol
CAP	Huawei Concurrence Accelerate Platform architectural component.
CLI	Command Line Interface
ESP	Encapsulated Security Payload (a subset of IPsec, Internet Protocol Security)
EXEC	Linux command for invoking subprocess(es)
GUI	Graphical User Interface
IETF	Internet Engineering Task Force, a standards body
IKE	Internet Key Agreement, a key agreement scheme associated with IPsec
IPC	Inter-process communication
IPS	Intrusion Prevention System
Ipsec	Internet Protocol Security (IPsec) as defined by the IETF
LDAP	Lightweight Directory Access Protocol
LOG	Linux Logging Service
NAT	Network Address Translation
POST	Power-on Self-tests
QOS	Quality of service
RFC	Request For Comment; the prefix used by IETF for internet specifications.
SSH	Secure Shell

Term	Definition
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRP	Huawei Versatile Routing Platform architectural component
VTY	Virtual Terminal (CLI created via Telnet)

Table 2 – Acronyms and Definitions (for terms not defined in FIPS 140-2 and associated documents)

1 Introduction

The Huawei R230D, R240D, R250D Remote Radio Units ("R Series Wlan" or "the modules") are multi-chip standalone cryptographic modules enclosed in hard, commercial grade plastic cases. The cryptographic boundary for these modules is the enclosure. The primary purpose of these modules is to provide secure communication for data transmitted between different networks. The modules provide network interfaces for data input and output. The appliance encryption technology uses FIPS approved algorithms. FIPS approved algorithms are approved by the U.S. government for protecting Unclassified data.

	HW Version	FW Version
Modules	R230D	V200R007C10SPC100
	R240D	V200R007C10SPC100
	R250D	V200R007C10SPC100
Tamper-evident seals and stickers	4057-113016	N/A

Table 3 – Cryptographic Module Configurations

The FIPS 140-2 security levels for the module are as follows:

Security Requirement	Security Level
Overall	**2**
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 4 – Security Level of Security Requirements

1.1 Module Architecture

The modules are constructed from standard production quality parts. The modules are classified as a multi-chip standalone cryptographic modules and are enclosed in hard, commercial grade plastic cases. The cryptographic boundary for these modules is the enclosure. The modules are designated as utilizing a non-modifiable operational environment under the FIPS 140-2 definitions. Any other firmware loaded

into this module is out of the scope of this validation and require a separate FIPS 140-2 validation. The following diagram shows the major architectural components of the module.

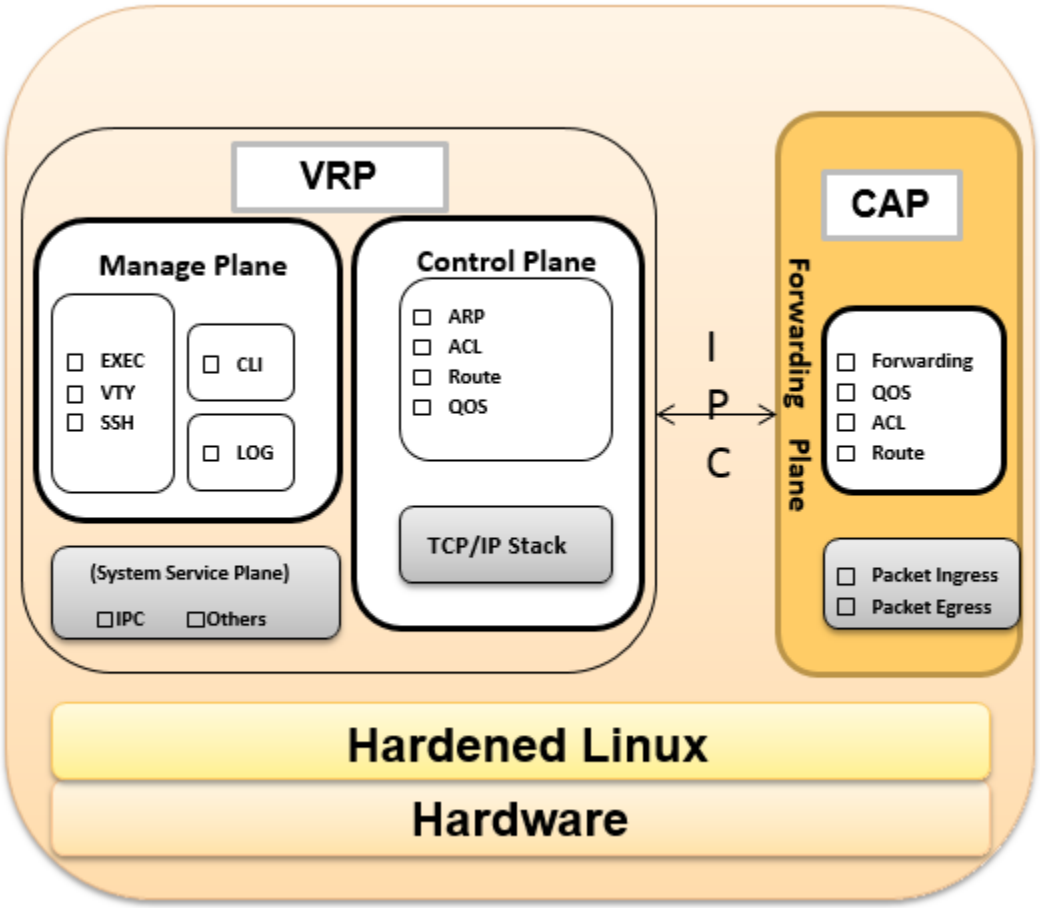


Figure 1 –R Series Architectural Block Diagram

1.2 Hardware

R Series Wlan provide a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four (4) FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output.

Figures of tamper-evident seal placement refer to Section 5.1.

The logical interfaces and their mapping are described in the following tables:

Figure 2 – R230D Physical Form

Port	Description	Logical Interface Type
1. ETH/PoE	Network traffic (10/100BASE-T) , connects to the central AP and supports PoE power input.	Control in, Data in, Data out, Status out, Power in
2. Default	Restores factory settings if you hold down the button more than 3s.	Control in
Internal antenna	A 2.4GHz/5GHz dual-band antenna to send and receive service signals.	Control in, Data in, Data out, Status out

Table 5 –R230D Ports and Interfaces

The following R230D components are used for signal conditioning and their identity cannot be used to compromise the security of the module. Therefore, they are not security relevant and are excluded from the requirements of FIPS 140-2.

- Capacitor (ref. des. C9, C15 - C17, C44 - C48, C52 - C58, C61, C62, C66, C69, C72 - C75, C77 - C82, C84 - C87, C89 - C91, C93 - C98, C100 - C106, C153 - C167, C169, C170, C178, C179, C181, C184 - C189, C191 - C194, C199 – C201, C208, C209, C322 - C324)
- Diode (ref. des. U1, VD2, VD3)
- Ground test point
- IC (ref. des. U18)
- Inductor (ref. des. L2, L7, U19)
- Reserved pads (ref. des. C11, C20, C107, C244, C259, C248, C291, C334, C336, U16, R91)
- Resistor (ref. des. R2, R7, R8, R46, R47, R51, R54, R73, R76, R81, R100, R101, R108, R119, R124, R143, R144, R215, R319)
- Switch (ref. des. S1)
- Transistor (ref. des. VT5)
- Transformer (ref. des. U21)
- EMI beads (ref. des. R202, R203)

Figure 3 – R240D Physical Form

Port	Description	Logical Interface Type
1. Eth Mgmt	Network traffic 1-4 (10/100BASE-T), connects to the wired Ethernet. Seen from the bottom, the four Ethernet interfaces are ETH0, ETH1, ETH2, and ETH3 from left to right.	Control in, Data in, Data out, Status out
2&4. Phone	Phone interface: connects to a traditional PSTN.	Data in, Data out, Status out
3. GE/PoE	Network traffic 1-4 (10/100/1000BASE-T) , connects to the central AP and supports PoE power input.	Control in, Data in, Data out, Status out, Power in
5. Default	Restores factory settings if you hold down the button more than 3s.	Control in
6. Power	Use a DC power cable to connect the Wlan to an external power source.	Power in
Internal antenna	A 2.4GHz/5GHz dual-band antenna to send and receive service signals.	Control in, Data in, Data out, Status out

Table 6 –R240D Ports and Interfaces

The following R240D components are used for signal conditioning and their identity cannot be used to compromise the security of the module. Therefore, they are not security relevant and are excluded from the requirements of FIPS 140-2.

- Capacitor (ref. des. C393, C454, C455, C460, C461, C465, C466, C481)
- IC (ref. des. U8)
- Inductor (ref. des. L10)
- Reserved pads (ref. des. F7, J10, C392)

- Resistor (ref. des. R372, R376 - R379)
- Transistor (ref. des. Q5)
- Transformer (ref. des. T2)

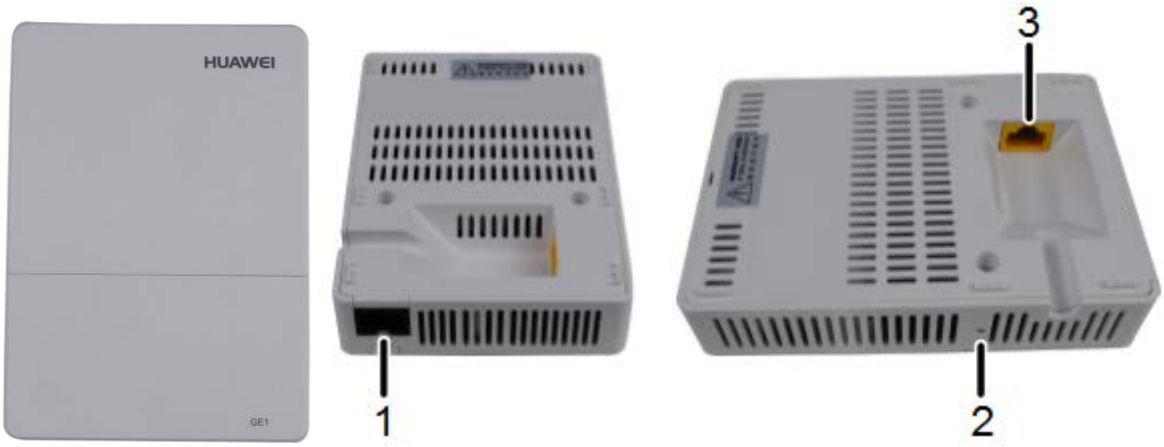


Figure 4 – R250D Physical Form

Port	Description	**Logical Interface Type**
1. GE1	Network traffic (10/100BASE-T), connects to the wired Ethernet.	Control in, Data in, Data out, Status out
2. Default	Restores factory settings if you hold down the button more than 3s.	Control in
3. GE0/PoE_IN	Network traffic (10/100/1000BASE-T) , connects to the central AP and supports PoE power input.	Control in, Data in, Data out, Status out, Power in
Internal antenna	A 2.4GHz/5GHz dual-band antenna to send and receive service signals.	Control in, Data in, Data out, Status out

Table 7 –R250D Ports and Interfaces

The following R250D components are used for signal conditioning and their identity cannot be used to compromise the security of the module. Therefore, they are not security relevant and are excluded from the requirements of FIPS 140-2.

- Capacitor (ref. des. C44, C143, C144, C147, C148, C152, C153, C155, C158 – C167, C169 - C173, C178, C180, C182, C185 – C194, C255, C271)
- Diode (ref. des. U16, U18)
- Ground pads and test points (incl. J2, TP33)
- Reserved pads (ref. des. C133, C243, C373, C627, C635, R453, R462)
- Resistor (ref. des. R100 - R104, R123, R175, R423, R449, R464, R458, R811, R818)
- Transistor (ref. des. VT1)
- Transformer (ref. des. T2)
- EMI beads (ref. des. L14)

1.3 Modes of Operation

The module supports both an Approved and non-Approved mode of operation. By default, the module comes configured in the non-Approved mode. In the Approved mode, only the services listed in Tables 14 and 15 are available; further, the Establish SSH service is constrained to use only the SSH options listed in the first column of Table 8. In the non-approved mode, all services in Tables 14, 15, and 16 are available for use, and all SSH options from Table 8 are available.

See Section 8, *Security Rules and Guidance*, for instructions on how to configure the module to function in the Approved mode operation.

2 Cryptographic Functionality

The cryptographic protocols and primitves implemented and used by the modules are listed in this section. Table 8 lists the SSH security methods; SSH methods are independently selectable and may be used in any combination.

The module uses SSHv2 to provide a shell interface over Ethernet for module configuration and administration.

Key Exchange
diffie-hellman-group14-sha1
Server Host Key (Authentication)
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
Digest
hmac-sha2-256
hmac-sha1
hmac-sha1-96
Cipher
aes128-cbc
TDES-CBC

Key Exchange
diffie-hellman-group1-sha1
diffie-hellman-group-exchange-sha1
Server Host Key (Authentication)
ssh-dss
ssh-rsa
Digest
hmac-md5
hmac-md5-96
Cipher
DES CBC
aes128-ctr
aes256-ctr
aes256-cbc

Table 8 – SSH Security Methods Available (Left: Both modes; Right: non-Approved mode only)

In the non-Approved mode, the module also supports SSH v1.5 with the same set of algorithms listed above.

Table 9, Table 10, and Table 11 lists all Approved, Allowed and non-Approved algorithms used by the library, respectively.

CAVP	Algorithm	Standard	Mode/Method	Strength[1]	Use
4408	AES	FIPS 197, SP 800-38A	CBC	128[2]	Data Encryption/Decryption
Vendor Affirmed	CKG	SP800-133	N/A		Key Generation
1114	CVL (SSH[3] KDF)	SP 800-135	SHA-1		KDF used to derive SSH v2 session keys
1421	DRBG[4]	SP 800-90A	HASH_DRBG	256	Deterministic Random Bit Generation
1060	ECDSA	FIPS 186-4	P-256 (SHA-256), P-384 (SHA-384), P-521 (SHA-512)		ECDSA Key generation; Digital Signature Generation/Verification
2930	HMAC	FIPS 198-1	HMAC-SHA-1-96 HMAC-SHA-1 HMAC-SHA-256		Message Authentication
3634	SHS	FIPS 180-4	SHA-1,SHA-256 , SHA-384, SHA-512		Message Digest Generation
2375	Triple-DES[5]	SP 800-67	TCBC	112	Data Encryption/Decryption for SSH

Table 9 - Approved Algorithms

[1] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli
[2] Key sizes 192 and 256 are only used when running a self-test
[3] No parts of the SSH protocol, other than the KDF, have been tested by the CAVP and CMVP
[4] Prediction resistance; hash_df used for instantiation
[5] Keys used for SSH and generated as described by RFC 4253

Algorithm	(Establishment) Strength	Use
Non SP800-56A compliant Diffie-Hellman	DH Group 14 (2048-bit modulus) (key agreement; key establishment methodology provides 112 bits of encryption strength)	Key establishment
NDRNG	Internal entropy source with rationale to support the claimed DRBG security strength.	DRBG (Cert. #1421) entropy input

Table 10 - Allowed Algorithms

Algorithm	Use
AES (non-compliant)	GCM & Keywrap Data Encryption/Decryption for CAPWAP
Blowfish	Message encryption in SSH
DES	Data Encryption/Decryption
DH Group 1	For key exchange within SSH
HMAC-MD5	For key exchange within SSH
MD5	Message Digest Generation
RSA (non-compliant)	SSH key establishment

Table 11 - Non-Approved Algorithms (Used only in the non-Approved Mode)

2.1 Critical Security Parameters and Public Keys

All CSPs used by the module are described in this section. All symmetric keys or generated seeds for asymmetric key generation are unmodified output from the DRBG.

Name	Description and usage
AUTH-PW	Authentication Passwords, minimum of 8 characters.
DRBG-EI	Entropy input (256 bytes) to the hash_df used to instantiate the Approved Hash_DRBG.
DRBG-STATE	SP 800-90A Hash_DRBG V and C values
SSH-DH	SSH Diffie-Hellman ephemeral private key used in SSH (n=2047).
SSH-Priv	SSH private key. ECDSA (P-256, P-384, P-521) private key used to establish SSH sessions.
SSH-SENC	SSH Session Encryption Key. AES-128 or 3-Key Triple-DES key for SSH message encrypt/decrypt.
SSH-SMAC	SSH Sesssion Authentication Key. HMAC-SHA1, HMAC-SHA1-96 and HMAC-SHA2-256 session key for SSH message authentication.

Table 12 – Critical Security Parameters (CSPs)

Name	Description and usage
SSH-Pub	SSH public key. ECDSA (P-256, P-384,P-521) public key used for SSH session establishment.
SSH-DH-Pub	SSH Diffie-Hellman public component. Ephemeral DH public key used in SSH. DH (L=2048 bit).

Table 13 – Public Keys

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module does not support a maintenance role or bypass capability. The module supports concurrent use via SSH. Authentication status does not persist across module power cycles. Upon authentication the user assumes both the Crypto Officer and Administrative User roles.

3.2 Authentication Methods

Authentication is performed by *password verification* and requires an eight (8) character minimum password using characters from at least two (2) categories of printable character sets (upper case, lower case, special character and numbers).

Hence the weakest password that meets the policy but whose components are still chosen randomly would be seven (7) digits and one upper or lower case character. This results in an upper bound probability of one in 2.6x10^8 which is less than one in 1,000,000.

After n consecutive unsuccessful authentication attempts, the module will lockout additional authentication requests for a minimum of five (5) minutes. The default value for n is 3, but per the security rules must be less than 2600.

The probability of false authentication in a one minute period is 2599/(2.6x10^8) = 1/100038

3.3 Services

All services implemented by the module are summarized next, with additional detail provided in Table 17 for traceability of cryptographic functionality and access to CSPs and public keys by services.

Service	Description
Configure System	File management, and logging configuration.
Configure Network	Network Interface configuration and management.
Module Reset	Reboot the module via reset CLI command. This service executes the suite of self-tests required by FIPS 140-2.
Status Monitoring and Reporting	Provides module status (CPU usage, etc.) and logs.
User Management and Authentication	Creating users and setting access rights.

Table 14 – Authenticated Module Services

Service	Description
Establish SSH	Establish an SSH session. Other services may be provided over SSH connection. In the approved mode, only the security methods in the first column of Table 8 may be used. In the non-Approved mode, all methods in Table 8 may be used.
Network Traffic	Provides network services through WAN, Uni/Multicast routing, QoS, Ethernet switching, IP services(DHCP, DNS).
Reset to Factory	This restores the module to factory defaults and is the means of providing zeroization of some CSPs
Show Status	This service provides the current status of the cryptographic module, indicators on the device show the module running properly or restarting

Table 15 – Unauthenticated Module Services

Service	Description
CAPWAP	Control And Provisioning of Wireless Access Points Protocol Specification
Ftp	File Transfer Protocol
Remote AAA	Connection to remote AAA server (RADIUS, TACACS)
Telnet	Using telnet to remotely manage and maintain several devices without the need to connect each device to a terminal, data is transmitted using TCP in plain text

Table 16 –Services only available in Non-FIPS mode

The next table defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.

- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
  Z = Zeroize: The module zeroizes the CSP.

Services	AUTH-PW	DRBG-EI	DRBG-STATE	SSH-DH	SSH-Priv	SSH-SENC	SSH-SMAC	SSH-Pub	SSH-DH-Pub
Unauthenticated									
Establish SSH	--	GE	GE	GE	RE	GE	GE	RE	GE
Network Traffic Management	--	--	--	--	--	--	--	--	--
Reset to Factory	WZ	Z	Z	Z	--	Z	Z	--	Z
Show Status	--	--	--	--	--	--	--	--	--
Authenticated (CO/User)									
Configure System	RE	GE	GE	--	GRE	GREWZ	GREWZ	GRE	GREWZ
Configure Network	RE	GE	GE	--	GWZ	--	--	GWZ	--
Module Reset	RE	Z	Z	Z	--	Z	Z	--	Z
Status Monitoring and Reporting	RE	--	--	--	--	--	--	--	--
User Management and Authentication	RWEZ	--	--	--	--	--	--	--	--

Table 17 – CSP Access Rights within Services

4 Self-tests

Each time the module is powered up it tests the integrity of the firmware and that the cryptographic algorithms still operate correctly. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the module automatically performs the self tests described in Table 18 below. All KATs must be completed successfully prior to any other use of cryptography by the module. Once called, the initialization function does not allow any user intervention.

All data output via the data output interface is inhibited when an error state exists and during self-tests. Upon successful completion of the self-test the moudules SYS_LED will go from steady on green to flash in green at 4Hz. If a failure of a self-test occurs,the module enters an error state, the modules SYS_LED will go from steady on green to falsh in Red at 4Hz for 9mins and then reboot. Upon failure of self-test three times, modules switch to boot back-up firmware.

Test Target (Cert. #)	Description
Firmware Integrity	32 bit CRC performed over all code in Flash
AES (#4408)	Separate encrypt and decrypt KATs using 128-bit keys and CBC mode Separate encrypt and decrypt KATs using 192-bit keys and CBC mode Separate encrypt and decrypt KATs using 256-bit keys and CBC mode
Triple DES (#2375)	Separate encrypt and decrypt KATs using 3 different keys and CBC mode
DRBG (#1421)	SHA-256 DRBG Health test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90A, Rev 1 Section 11
HMAC (#2930)	Separate HMAC generation and verification KATs, using SHA-1 Separate HMAC generation and verification KATs, using SHA-256
ECDSA (#1060)	Roundtrip signature and verification
SHS (#3634)	Separate KAT of SHA-1 and SHA-512 (SHA-256 tested in HMAC KATs)

Table 18 – Power Up Self-tests

Test Target	Description
NDRNG	AS09.42 Continuous RNG Test performed on each NDRNG access
ECDSA	Pairwise Consistency Test using private key for signature generation and public key for signature verification

Table 19 – Conditional Self-tests

5 Physical Security Policy

The cryptographic modules each include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper-evident material and tamper-evident seals
- Opacity stickers

An operator in the CO role is responsible for the following:

- Applying the tamper seals per Section 5.1 below. The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. The CO is responsible for having control at all times of any unused seals.
- Inspecting the tamper-evident seals based on the schedule described in Table 20 below.
- If the module shows signs of tampering, the CO should zeroize the module and contact the manufacturer.

Mechanism	Recommended Frequency of Inspection/Test
Tamper-evident Seals	Inspect tamper-evident seals monthly.
Opacity Stickers	Inspect opacity stickers monthly

Table 20 – Physical Security Inspection Guidelines

5.1 Tamper Seal Placement

The CO should ensure the module enclosure surface is clean and dry prior to the application of seals. The module contains tamper-evident seals and opacity stickers (as applicable), which are applied to each module as follows:

Figures 5-1 shows the installation locations of the 7 tamper seals and 3 opacity stickers for the R230D.

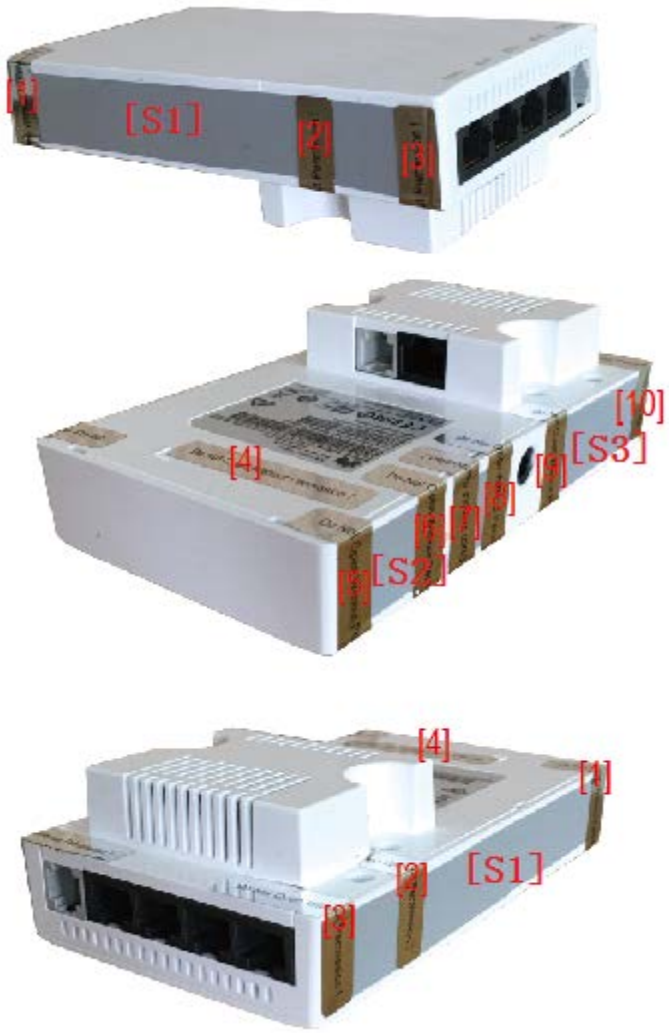
- [1] [4]: Cover the top and the side of the chassis.
- [3] [5]: Cover the top, bottom, and the side of the chassis.
- [2] [6]: Cover the bottom and the side of the chassis.
- [7]: Directly covers the heat dissipation holes on the bottom of the AP.
- [S1] [S2] [S3] : These opacity stickers cover the heat dissipation holes on the left and right sides of the AP.

Figures 5-1 R230D tamper seal placement

Figure 5-2 shows the installation locations of the 10 tamper seals and 3 opacity stickers for the R240D.

- [1] [5] [6] [7] [8] [9]: Cover the top, bottom, and the side of the chassis.
- [2] [3] [10]: Cover the bottom and the side of the chassis.
- [4]: Directly covers the heat dissipation holes on the bottom sides of the AP.
- [S1] [S2] [S3] : These opacity stickers cover the heat dissipation holes on the left and right sides of the AP.

Figures 5-2 R240D tamper seal placement



Figures 5-3 shows the installation locations of the 12 tamper seals and 3 opacity stickers for the R250D.

- [1] [7]: Cover the rear and the side of the chassis.
- [2] [3] [8]: Cover the top, bottom, and the side of the chassis.
- [4] [10] [11]: Cover the top and the side of the chassis.

- [5][6][12]: Directly cover the heat dissipation holes on the bottom, left, and right sides of the AP.
- [9]: Cover the bottom and the side of the chassis.
- [S1] [S2] [S3] : These opacity stickers cover the heat dissipation holes on the left and right sides of the AP.

Figures 5-3 R250D tamper seal placement

NOTE

After the CO applies the opacity stickers, the operational temperature range of the R230D/R240D/R250D will be 0°C to +40°C.

6 Operational Environment

The module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions; there is no mechanism for updating the module firmware.

7 Mitigation of Other Attacks Policy

The modules have not been designed to mitigate attacks outside the scope of FIPS 140-2.

8 Security Rules and Guidance

1. An unauthenticated operator does not have access to any CSPs or cryptographic services.
2. The module inhibits data output during power up self-tests and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. The operator shall remain in control of the module until the zeroization process completes. Zeroization overwrites all CSPs and is performed performed with the following procedure:
   - Zeroize the ECC key pair using the "ecc local-key-pair destroy" command.
   - Reset to factory settings using the "reset factory configuration" command.
5. The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation.

The following security rules must be adhered to for operation in the FIPS 140-2 Approved mode:

6. Upon first time initialization, the User shall authenticate to the module using the default username and password:

   Username: admin
   Password: admin@huawei.com
7. Place the module in the Approved mode of operation by issuing the following command: “set workmode fips enable”.
8. When faced with the following prompt: “Successfully set fips mode will reboot the system. Continue”? Enter ‘y’ to continue. The module will then save the workmode flag in flash, zeroize, and automatically reboot in FIPS mode.
9. Upon the reboot the CO shall authenticate and update the default password for the boot menu and the SSH interface. The minimum password strength is enforced by the module per Section 3.2. The CO can proceed with module configuration per the vendor provided Configuration Guide (available here: http://support.huawei.com/enterprise/en/wlan/ r200-pid-22039811).
10. The CO must not configure the failed authentication limit setting to more than 2599.
11. When switching modes, the CO shall follow the zeroization procedure.

An operator of the module can determine if the module is running the Approved mode of operation by adhering to the above rules.