Huawei AR2240, AR3260 and AR169FGVW-L Series Routers

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.2

Date: July 17, 2017

Contents

Tables

Figures

References and Definitions

Table 1: References

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

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	Concurrence Accelerate Platform
CLI	Command Line Interface
ESP	Encapsulated Security Payload (a subset of IPsec, Internet Protocol Security)
GUI	Graphical User Interface
HFCL	Huawei FIPS Cryptographic Library
IETF	Internet Engineering Task Force, a standards body
IKE	Internet Key Agreement, a key agreement scheme associated with IPsec (but not used by the module)
IPC	Inter-process Communication
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol
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.
SIC	Service Interface Card

Term	Definition
SRU	Switching and Routing Unit
SSH	Secure Shell
TLS	Transport Layer Security
TSM	Terminal Security Management
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRP	Versatile Routing Platform
VTY	Virtual Terminal Line
WSIC	Wide Service Interface Card
XSIC	Extended Service Interface Card

1 Introduction

The Huawei AR2240, AR3260 and AR169FGVW-L Series Routers are multi-chip standalone cryptographic modules enclosed in hard, commercial grade metal cases. The cryptographic boundary for these modules is the enclosure. The primary purpose of these modules is to integrate multiple services including; routing, switching, 3G, voice, and security functions in one device. 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.

The module is designated as 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.

Table 3: Cryptographic Module Configurations

	Base Model[1]	HW Version	Tamper Seals	External Baffle	FW Version
1	AR2240	P/N 03022UFU Version C.2	P/N 4057-113016	P/N 99089JEB	V200R008C10SPC120
2	AR3260	P/N 03022NPN Version I.3	P/N 4057-113016	P/N 99089JEB	V200R008C10SPC120
3	AR169FGVW-L	P/N 50010168 Version L.2	P/N 4057-113016	P/N 99089JEB	V200R008C10SPC120

Figure 1 - Figure 6 show the cryptographic boundary of the module.

Figure 1: AR2240 (Top, Right, Front)

[1] Note that the FIPS validated configuration is the base model with no interface cards installed.

Figure 2: AR2240 (Bottom, Left, Back)

Figure 3: AR3260 (Top, Right, Front)

Figure 4: AR3260 (Bottom, Left, Back)

Figure 5: AR169FGVW-L (Top, Right, Front)

Figure 6: AR169FGVW-L (Bottom, Left, Back)

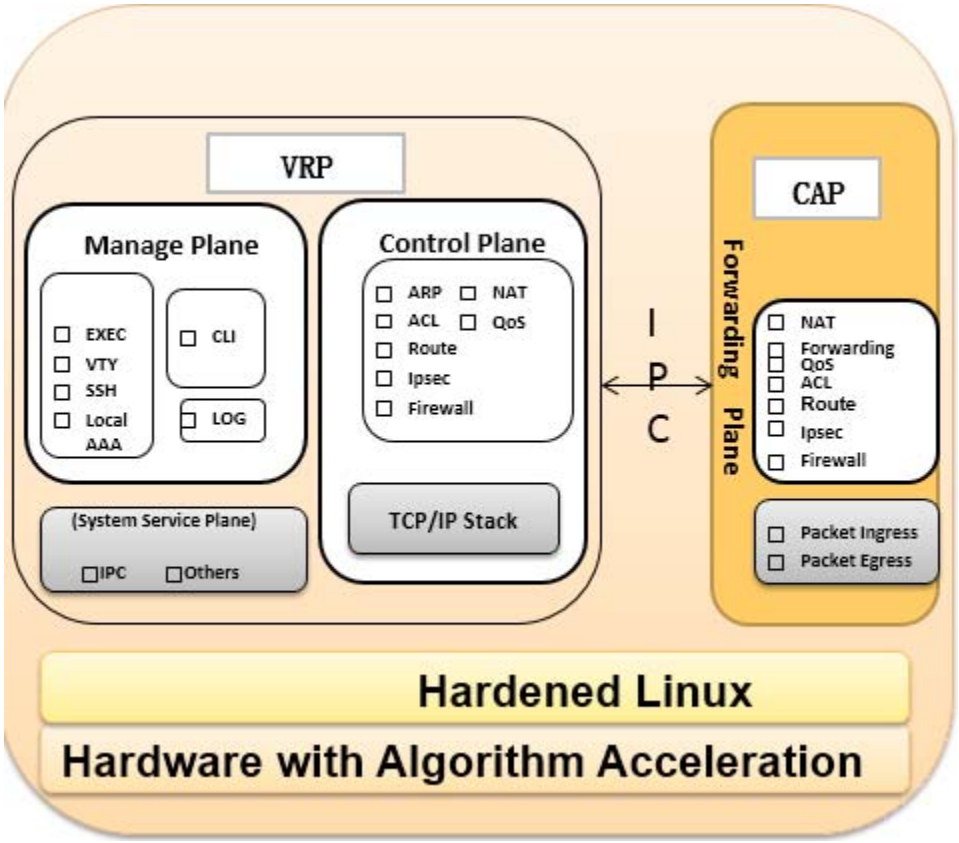

Figure 7: Firmware Block Diagram

1.1 Security Levels

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

Table 4: Security Level of Security Requirements

Security Requirement	Security Level
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

1.2 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.

See Section 9, *Security Rules and Guidance*, for instructions on how to configure the module to function in the Approved mode operation.

2 Ports and Interfaces

The modules provide a number of physical interfaces, and these are mapped to the four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in Table 5.

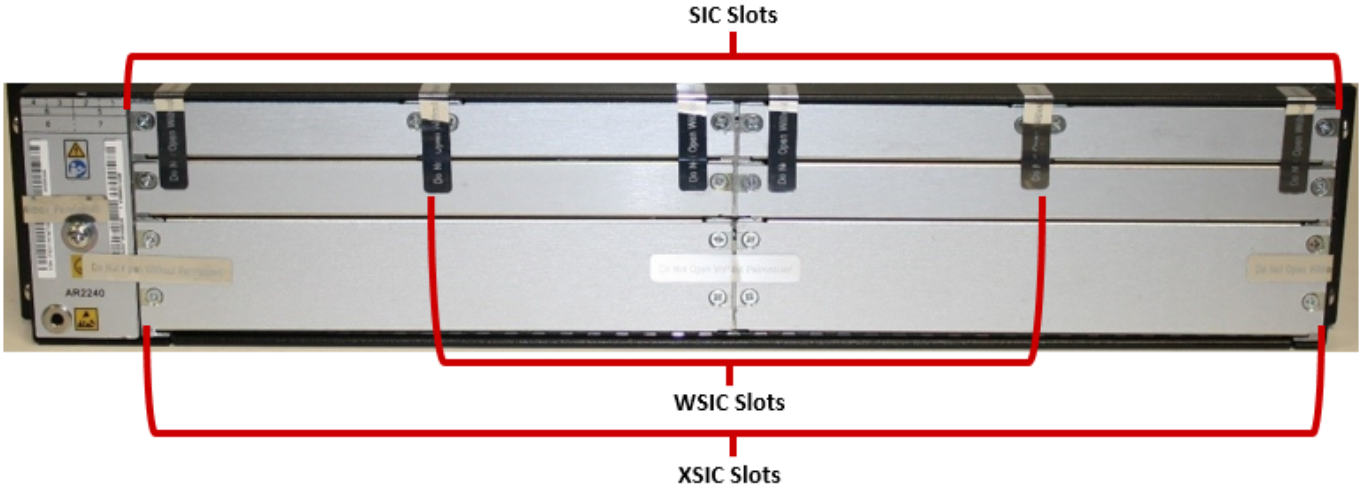

Figure 8: AR2240 Front Panel Ports/Interfaces

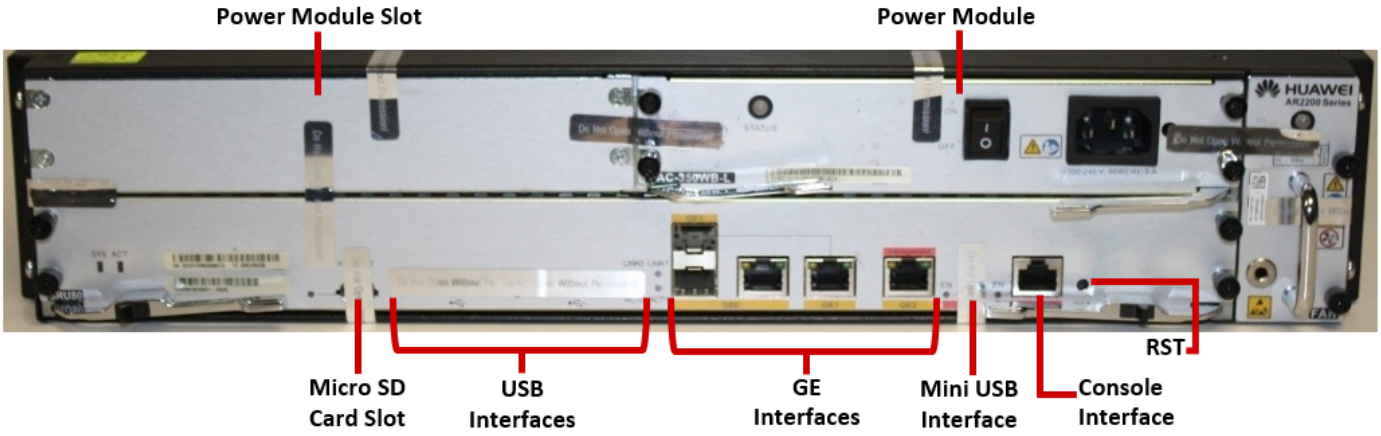

Figure 9: AR2240 Back Panel Ports/Interfaces

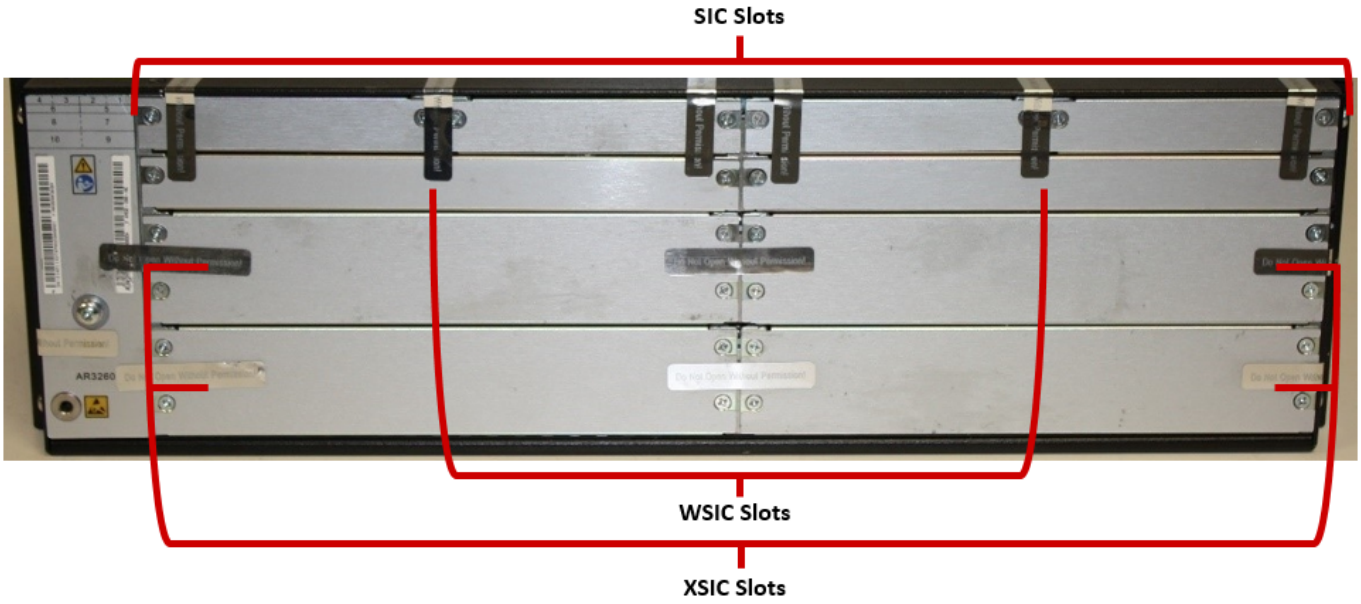

Figure 10: AR3260 Front Panel Ports/Interfaces

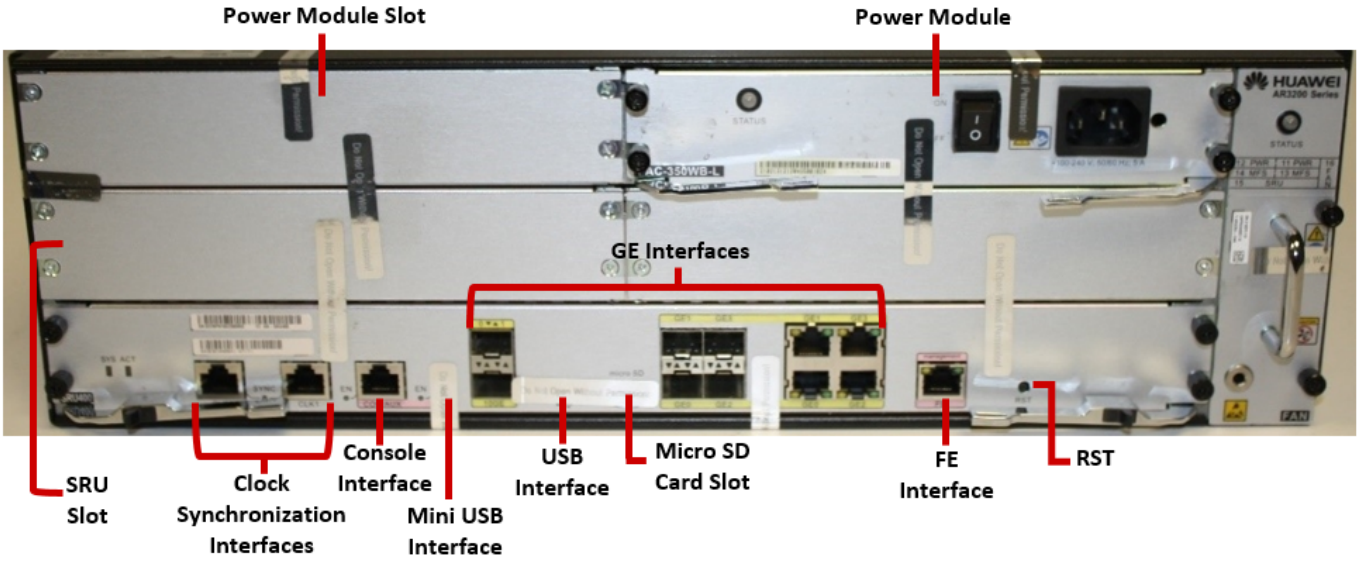

Figure 11: AR3260 Back Panel Ports/Interfaces

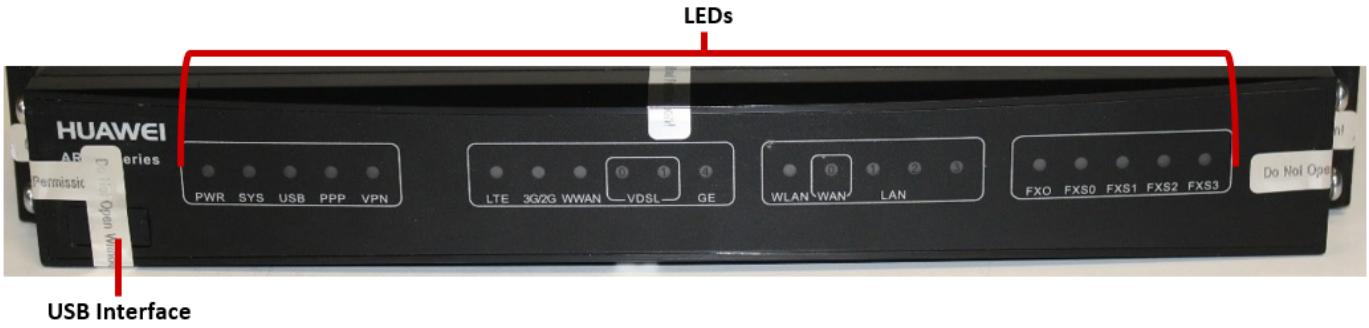

Figure 12: AR169FGVW-L Front Panel Ports/Interfaces

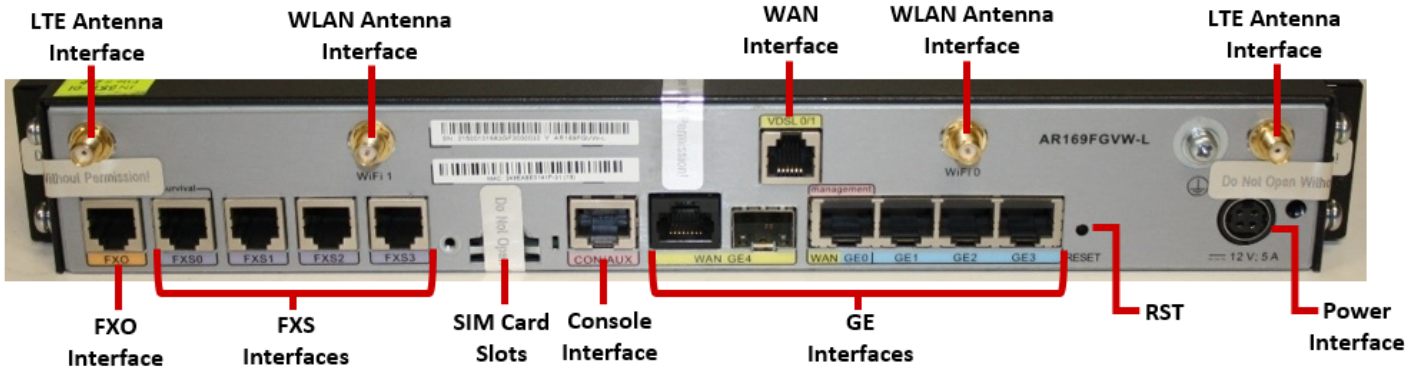

Figure 13: AR169FGVW-L Back Panel Ports/Interfaces

Table 5: Ports and interfaces

Quantity			Port	Description	Logical Interface Type
AR2240	AR3260	AR169			
2	1	1	USB	USB interface	N/A – Covered with tamper evident seal
1	1	--	Mini USB	Mini USB interface	N/A – Covered with tamper evident seal
1	1	--	MicroSD	Micro SD card slot	N/A – Covered with tamper evident seal
1	1	1	RST	Reset button	Control in
1	1	1	Console	Serial console	Control in, data in, data out, status out
5	10	6	GE Interface	Network traffic connection	Control in, data in, data out, status out
--	1	--	FE Interface	Management Interface	Control in, data in, data out, status out

Quantity			Port	Description	Logical Interface Type
AR2240	AR3260	AR169			
--	--	1	FXO Interface	Can be connected to a public switched telephone network (PSTN) using a standard telephone cable	Data in, data out
--	--	4	FXS Interface	Can be connected to analog telephones using standard telephone cables	Data in, data out
--	--	2	WLAN Antenna Interface	Wi-Fi interface to transmit and receive data	N/A - Disabled in firmware
--	--	2	LTE Antenna Interface	LTE interface to transmit and receive data	N/A - Disabled in firmware
--	--	1	WAN Interface	VDSL 0/1 interface	Control in, data in, data out, status out
--	2	--	Clock Synchronization interface	Reserved interfaces	N/A - The router does not support clock synchronization currently.
--	--	1	AC Power Interface	Power jack	Power
1	1	--	Power Module	Power plug and switch	Power
1	1	--	Power Module Slot	Additional power module Slot (AC, DC, AC PoE)	N/A – Populated with a faceplate and secured in place with tamper evident seals
4	4	--	SIC Slots	Service Interface Card slots and connector	N/A – Populated with a faceplate and secured in place with tamper evident seals
2	2	--	WSIC Slots	Wide Service Interface Card slots and connector	N/A – Populated with a faceplate and secured in place with tamper evident seals
2	4	--	XSIC Slots	Double Height Wide Service Interface Card slots and connector	N/A – Populated with a faceplate and secured in place with tamper evident seals
--	1	--	SRU Slot	Additional Switching and Routing Unit slot	N/A – Populated with a faceplate and secured in place with tamper evident seals
--	--	2	SIM card slots	For mounting SIM cards	N/A – Covered with tamper evident seal
13	16	21	LEDs	USB, SYS, Network traffic LEDs, etc.	Status out

3 Cryptographic Functionality

The cryptographic protocols and primitives implemented and used by the modules are listed in this section. Table 6 lists the SSH security methods; SSH methods are independently selectable and may be used in any combination. Table 7 lists the IPsec security methods.

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 SSHv2 service is constrained to use only the Approved SSH options listed in Table 6. In the non-Approved mode, all services in Tables 14, 15 and 16 are available for use, and all SSH options from Tables 6 are available.

The module uses SSH-2 to provide a shell interface over Ethernet for module configuration and administration.

Table 6: SSH Security Methods Available in Each Mode

SSH Security Methods	Approved Mode	Non-Approved Mode
Key Exchange		
diffie-hellman-group14-sha1	X	X
Server Host Key (Authentication)		
ssh-ecdsa	X	X
Digest		
hmac-md5-96		X
hmac-sha1	X	X
hmac-sha1-96	X	X
Cipher		
des-cbc		X
aes128-cbc	X	X
blowfish-cbc		X
3des-cbc	X	X

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

The module uses IPsec ESP mode for data transport, using AES-128, AES-192 and AES-256 in CBC mode with IKE v2 key exchange. Only Oakley Group 14 is used by the IKE key exchange.

Table 7: IPsec ESP Cipher and Digest Methods Available

Cipher Suite String (IETF enumeration)	Cipher	Digest
AES128-CBC-SHA	AES-128	SHA-1
AES128-CBC-SHA256	AES-128	SHA-256
AES128-CBC-SHA384	AES-128	SHA-384
AES128-CBC-SHA512	AES-128	SHA-512
AES192-CBC-SHA	AES-192	SHA-1
AES192-CBC-SHA256	AES-192	SHA-256
AES192-CBC-SHA384	AES-192	SHA-384
AES192-CBC-SHA512	AES-192	SHA-512

Cipher Suite String (IETF enumeration)	Cipher	Digest
AES256-CBC-SHA	AES-256	SHA-1
AES256-CBC-SHA256	AES-256	SHA-256
AES256-CBC-SHA384	AES-256	SHA-384
AES256-CBC-SHA512	AES-256	SHA-512
3DES-CBC-SHA	3DES	SHA-1
3DES-CBC-SHA256	3DES	SHA-256
3DES-CBC-SHA384	3DES	SHA-384
3DES-CBC-SHA512	3DES	SHA-512

Table 8, Table 9 and Table 10 list all Approved, Allowed and non-Approved algorithms used by the library, respectively.

Table 8: Approved Algorithms

CAVP	Algorithm	Standard	Mode/Method	Strength[2]	Use
Library: HFCL					
4323	AES	FIPS 197, SP 800-38A	CBC	128, 192, 256	Data Encryption/ Decryption
Vendor affirmed	CKG	SP 800-133	N/A	N/A	Key Generation
1036 (CVL)	SSH[3] KDF	SP 800-135	SHA-1		KDF used to derive SSH v2 session keys
	IKE[3] KDFs	SP 800-135	2048: SHA-1, SHA-256, SHA-384, SHA-512		KDF used to derive IKEv2 session keys
1379	DRBG[4]	SP 800-90A	Hash_DRBG	256	Deterministic Random Bit Generation
1023	ECDSA	FIPS186-4	P-224 and P-256 (SHA-256)		ECC Key Generation; Digital Signature Generation/ Verification
2861	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512		Message Authentication
(based on 2861)	HMAC	IG A.8	HMAC SHA-1-96		Message Authentication in SSH
4323 2861	KTS: AES HMAC	SP 800-38F	Key Wrap		128
2335 2861	KTS: Triple-DES HMAC	SP 800-38F	Key Wrap		112
3565	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest Generation

[2] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli
[3] The SSH and IKE v2 protocols have not been reviewed or tested by the CAVP and CMVP.
[4] Prediction resistance; hash_df used for instantiation

CAVP	Algorithm	Standard	Mode/Method	Strength[2]	Use
Library: HFCL					
2335	Triple-DES	SP 800-67	TCBC	3-Key	Data Encryption/ Decryption

Table 9: Allowed Algorithms

Algorithm	(Establishment) Strength	Use
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. #1379) entropy input

Table 10: Non-Approved Algorithms (Used only in the non-Approved Mode)

Algorithm	Use
Blowfish	Message encryption in SSH
MD5	Message Digest Generation
HMAC-MD5	Message authentication
DES	Data Encryption/Decryption
DH Group 1 (768-bit modulus)	For key exchange within SSH, IPsec
DH Group 2 (1024-bit modulus)	For key exchange within IPsec
DH Group 5 (1536-bit modulus)	For key exchange within IPsec
SM3	Message Digest Generation
SM1	Data Encryption/Decryption
SM4	Data Encryption/Decryption
SNMP KDF (non-compliant)	KDF used to derive SNMP session keys[5]
IKEv1 KDF (non-compliant)	Key exchange within IPsec[5]

3.1 Critical Security Parameters and Public Keys

All CSPs used by the module are described in this section.

Table 11: Critical Security Parameters (CSPs)

Name	Description and usage
AUTH-PW	Authentication Passwords, minimum of 8 characters
DRBG-EI	Entropy input (1000 bytes) to the hash_df used to instantiate the Approved HASH_DRBG

[5] Keys derived from non-compliant protocols cannot be used in the Approved mode.

Name	Description and usage
DRBG-STATE	SP 800-90A Hash_DRBG V and C values (SHA-256, 440-bit V, per IG 14.5)
IKE-DH-PRIV	IKE ephemeral Diffie-Hellman private key for key exchange
IKE-MS	IKE master secret, used for SP 800-135 key derivation.
IKE-PSK	The IKE Pre-Shared Session: hmac-sha1, hmac-sha2-256, hmac-sha2-384, hmac-sha2-512.
IKE-SMAC	The IKE / IPsec session authentication key (two instances, one per each direction of communication): hmac-sha1, hmac-sha2-256, hmac-sha2-384, hmac-sha2-512.
IKE-SENC	The IKE / IPsec session encryption key (two instances, one per each direction): 3 Key Triple-DES, AES-128, AES-192, AES-256.
SSH-DH	SSH Diffie-Hellman private component (2048-bit). Ephemeral DH private key used in SSH.
SSH-Priv	SSH private key. ECDSA (P-224, P-256) 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 Session Authentication Key. HMAC-SHA-1 160-bit session key for SSH message authentication

Table 12: Public Keys

Name	Description and usage
SSH-Pub	SSH public key. ECDSA (P-224, P-256) 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)
IKE-PUB	IKE Diffie-Hellman public component. Ephemeral DH public key used in IKE. DH (L= 2048 bit)
IKE-PEER	IKE Diffie-Hellman public key provided by the IKE peer. DH (L=2048 bit)

4 Roles, Authentication and Services

4.1 Assumption of Roles

The module does not support a maintenance role or bypass capability. The module supports concurrent use by End Users and Administrators. The cryptographic module enforces the separation of roles by the partitioning of major subsystems (such as VPN traffic vs. shell or administrative functions), and by partitioning of the administrative interfaces. Authentication status does not persist across module power cycles. To change roles, an operator must first log out, then log in using another role.

Table 18 lists the available roles; the options for authentication type and data are common across roles.

Table 13: Roles Description

Role		Authentication	
ID	**Description**	**Type**	**Data**
Root Administrator (CO)	Cryptographic Officer – Has full access to administer and configure the module as well as delegate admin access control rights to Administrators.	Identity-based (using *Local password verification*)	Username and Password
Administrator (AD)	Configures and administers the module per the delegated access rights assigned by the Root Administrator.		
End User (EU)	Typical end user accessing the virtual private network resources via an encrypted connection.		

4.2 Authentication Methods

The *Local password verification* method, which includes IKE peer authentication, requires an 8 character minimum password using characters from at least two categories of printable character sets (upper case, lower case, special character and numbers).

Since there are 28 possible special characters and 26 upper or lower case characters, the weakest password that meets the policy but whose components are still chosen randomly would be 7 digits and one upper or lower case character. This results in an upper bound probability of (10^7) x 26. So, the probability of guessing the password with a single attempt is 1/(2.6x10^8) which is less than one in 1,000,000.

For SSH connections, after n consecutive unsuccessful authentication attempts, the module will lockout additional authentication requests for a minimum of 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

For console access, after 1 unsuccessful attempt, the module requires a waiting period of 5 seconds before accepting another authentication attempt. Thus, only 12 authentication attempts are possible over the console in a one minute period.

The probability of a false authentication in a one minute period is 12/(2.6x10^8), which is less than 1 in 100,000.

4.3 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.

Table 14: Authenticated Module Services

Service	Description	CO	AD	EU
Module Reset	Reboot the module via reset CLI command. This service executes the suite of self-tests required by FIPS 140-2.	X	X	
Configure System	License management, file management, and logging configuration.	X		
Configure Network	Network Interface configuration and management.	X	X	
Configure Policy	Configure VPN access policy.	X	X	
Status Monitoring and Reporting	Provides module status (CPU usage, etc.) and logs.	X	X	
User Management and Authentication	Creating users and setting access rights.	X	X[6]	
VPN	Provides VPN service through IPsec.			X
Firewall	Intrusion prevention and packet filtering.			X

(Note: This is a condensed list of services for the purposes of this Security Policy. The full list of module commands can be found in the module's User manual. The link to the User Manual is provided below in Section 8).

Table 15: Unauthenticated Module Services

Service	Description
Reset to Factory	This restores the module to factory defaults and is the means of providing zeroization of all keys and CSPs
Network Traffic Management	Provides network services through WAN, Uni/Multicast routing, QoS, Ethernet switching, IP services(DHCP, DNS, NAT) and Voice
Show Status	This service provides the current status of the cryptographic module, indicators on the device show the module running properly or restarting

Table 16: Services only available in Non-FIPS mode

Service	Description
Remote AAA	Connection to remote AAA server (RADIUS, TACACS)
SNMP	Configuration, administration and monitoring
RIP and RIPng	Routing protocol
OSPFv2 and OSPFv3	Routing protocol
ISIS and ISISv6	Routing protocol
BGP and BGP4+	Routing protocol
VRRP	Redundancy backup mechanism for IP services, including IPv4/IPv6 VRRP

[6]Only Administrators with a user level set between 3 and 15 can manage other administrator accounts

Service	Description
NTP	Time synchronization for traditional IP networks
L2TP	Functioning as the LAC or LNS and allowing concurrent user access on multiple channels
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 plaintext

Table 17 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.

Table 17: CSP and Public Key Access Rights within Services

Services	AUTH-PW	DRBG-EI	DRBG-STATE	IKE-DH-PRIV	IKE-MS	IKE-PSK	IKE-SMAC	IKE-SENC	SSH-DH	SSH-Priv	SSH-SENC	SSH-SMAC	SSH-Pub	SSH-DH-Pub	IKE-PUB	IKE-PEER
Unauthenticated																
Reset to Factory	WZ	Z	Z	Z	Z	WZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Network Traffic Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--		
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--		
Root Administrator (CO)																
Module Reset	--	GE	G	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	--	Z	Z
Configure System	E	--	EW	--	--	--	--	--	GRE WZ	GRE	GRE WZ	GRE WZ	GRE	GRE WZ		
Configure Network	--	--	EW	--	--	--	--	--	GRE WZ	--	GRE WZ	GRE WZ	--	GRE WZ		
Configure Policy	--	--	EW	--	--	RWZ	--	--	GRE WZ	--	GRE WZ	GRE WZ	--	GRE WZ		
Status Monitoring and Reporting	--	--	--	--	--	--	--	--	--	--	--	--	--	--		
User Management and Authentication	RWZ	--	--	--	--	--	--	--	--	--	--	--	--	--		
Administrator (AD)																
Module Reset	--	GE	G	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Configure Network	E	--	EW	--	--	--	--	--	GRE WZ	--	GRE WZ	GRE WZ	--	GRE WZ		
Configure Policy	--	--	EW	--	--	RWZ	--	--	GRE WZ	--	GRE WZ	GRE WZ	--	GRE WZ		

Services	AUTH-PW	DRBG-EI	DRBG-STATE	IKE-DH-PRIV	IKE-MS	IKE-PSK	IKE-SMAC	IKE-SENC	SSH-DH	SSH-Priv	SSH-SENC	SSH-SMAC	SSH-Pub	SSH-DH-Pub	IKE-PUB	IKE-PEER
Status Monitoring and Reporting	--	--	--	--	--	--	--	--	--	--	--	--	--	--		
User Management and Authentication	RWZ	--	--	--	--	--	--	--	--	--	--	--	--	--		
End User (EU)																
VPN	E	--	EW	GEZ	GEZ	E	GEZ	GEZ	--	--	--	--	--	--	GREWZ	EWZ
Firewall	--	--	--	--	--	--	--	--	--	--	--	--	--	--		

The *Module Reset* service instantiates the DRBG, with 1000 bytes entropy input (DRBG-EI) produced by the Allowed NDRNG. The generation of DRBG-STATE uses the [SP 800-90A] *Hash_df* with 519 bits of entropy input. Internally generated symmetric keys are the result of unmodified output from the DRBG. The Zeroization of session keys by this service covers the case of module shutdown or power-cycle while a secure channels session (SSH) is active.

The *Show Status* service does not access CSPs or public keys.

5 Self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the module performs the self tests described in Table 23 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-tests the modules SYS LED will go from Red to Green. If a failure of a self-test occurs, the module enters an error state, outputs the following error message on the console and forces the module to reboot: “Self-Test Fail…”

Table 18: Power Up Self-tests

Test Target (Cert. #)	Description
Firmware Integrity	32 bit CRC performed over all code
AES HFCL (#4323)	Separate encrypt, decrypt KATs using 128-bit keys and CBC mode Separate encrypt, decrypt KATs using 192-bit keys and CBC mode Separate encrypt, decrypt KATs using 256-bit keys and CBC mode
Triple DES HFCL (#2335)	Separate encrypt, decrypt KATs using 3 different keys and CBC mode
DRBG HFCL (#1379)	SHA-256 DRBG test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90A Section 11

Test Target (Cert. #)	Description
HMAC HFCL (#2861)	Separate HMAC generation and verification KATs, using SHA-1 Separate HMAC generation and verification KATs, using SHA-256 Separate HMAC generation and verification KATs, using SHA-384 Separate HMAC generation and verification KATs, using SHA-512
ECDSA HFCL (#1023)	Sign and verify Pairwise Consistency Test using P-224 and SHA-256
SHS HFCL (#3565)	Separate KAT of SHA-1 (SHA-256, SHA-384, SHA-512 tested in HMAC HFCL KATs)

Table 19: Conditional Self-tests

Test Target	Description
DRBG	AS09.42 Continuous RNG Test performed on each DRBG access
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

6 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 seals
- External baffles to provide opacity for the side vents

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

- Applying the tamper seals and baffles per Sections 6.1 and 6.2 below. The tamper evident seals and baffles 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 seals based on the schedule described in Table *20* below.

Table 20: Physical Security Inspection Guidelines

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

6.1 Baffle Installation

1) Install baffles on both left and right sides, and fasten each corner with screws (#1-4 in Figure 14).
2) Proceed in attaching the tamper seals per Section 6.2 below. Before attaching tamper seals, make sure that surfaces of the equipment are clean and dry.

Note that seals can be reordered from Huawei Technologies using the following part number: 4057-113016. This part number can be used to order any size baffle.

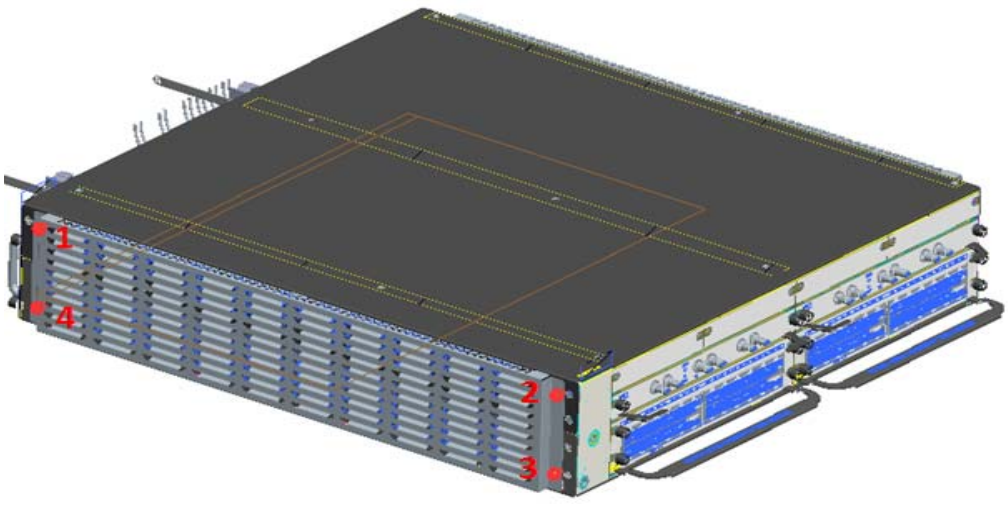

Figure 14: Baffle Locations – Left Side

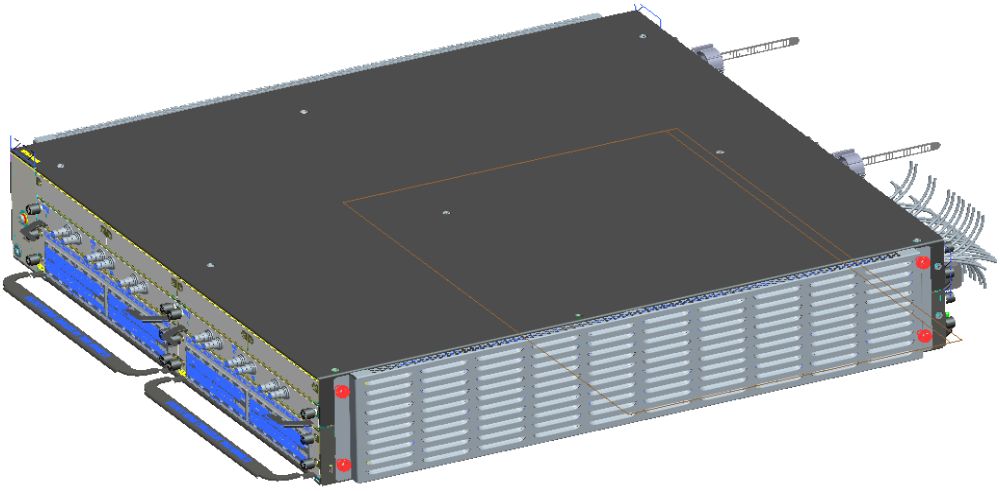

Figure 15: Baffle Locations – Right Side

6.2 Tamper Seal Placement

6.2.1 AR2240

The module includes twenty-five (25) tamper-evident seals, which are applied to the module as follows:

- One (1) seal applied to the front and left side, including the baffle (see #1 in Figure 16)
- Six (6) seals applied to the front top card plates and top (see #2 to #7 in Figure 16)
- Three (3) seals applied to the front card plates (see #8 & #10 in Figure 16)
- Two (2) seals applied to the back and each side, including the baffle (see #11 & #12 in Figure 17)
- Two (2) seals applied to the back and the top (see #13 & #14 in Figure 17)
- Three (3) seals applied to the back card plates, preventing removal (see #15 to #17 in Figure 17)
- One (1) seal applied to the back and bottom, preventing port access (see #18 in Figure 17)
- One (1) seal applied to the back and bottom (see #19 in Figure 17)
- Two (2) seals applied to the back, preventing port access (see #20 & #21 in Figure 17)
- Two (2) seals applied to the right side baffle and bottom/top preventing removal (see #22 & #23 in Figure 18)
- Two (2) seals applied to the left side baffle and bottom/top preventing removal (see #24 & #25 in Figure 19)

Figure 16: Front Plate Seals

Figure 17: Back Plate Seals

Figure 18: Right Side Plate Seals

Figure 19: Left Side Plate Seals

6.2.2 AR3260

The module includes twenty-eight (28) tamper-evident seals, which are applied to the module as follows:

- One (1) seal applied to the front and left side, including the baffle (see #1 in Figure 20)
- Six (6) seals applied to the front top card plates and top (see #2 to #7 in Figure 20)
- Six (6) seals applied to the front card plates (see #8 & #13 in Figure 20)
- Two (2) seals applied to the back and each side, including the baffle (see #14 & #15 in Figure 21)
- Two (2) seals applied to the back and the top (see #16 & #17 in Figure 21)
- Four (4) seals applied to the back card plates, preventing removal (see #18 to #21 in Figure 21)
- One (1) seal applied to the back, preventing port access (see #22 in Figure 21)
- One (1) seal applied to the back and bottom, preventing port access (see #23 in Figure 21)
- One (1) seal applied to the back and bottom (see #24 in Figure 21)
- Two (2) seals applied to the right side baffle and bottom/top, preventing removal (see #25 & #26 in Figure 22)
- Two (2) seals applied to the left side baffle and bottom/top, preventing removal (see #27 & #28 in Figure 23)

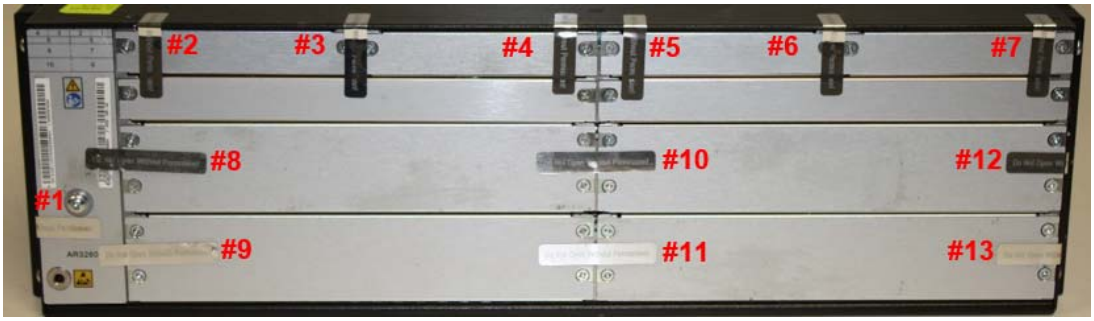

Figure 20: Front Plate Seals

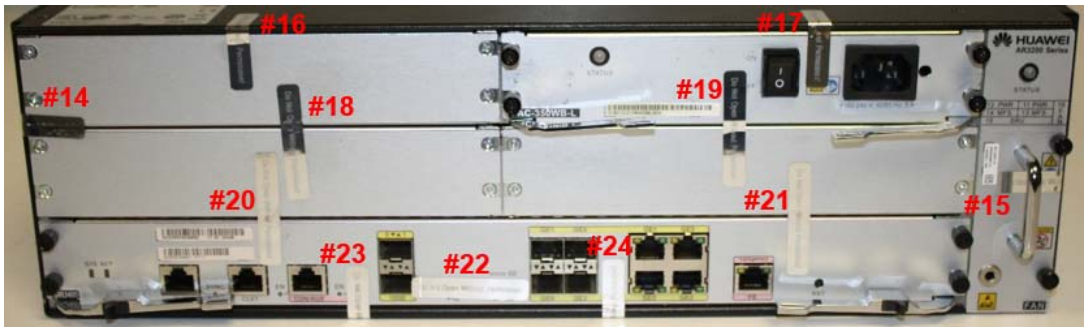

Figure 21: Back Plate Seals

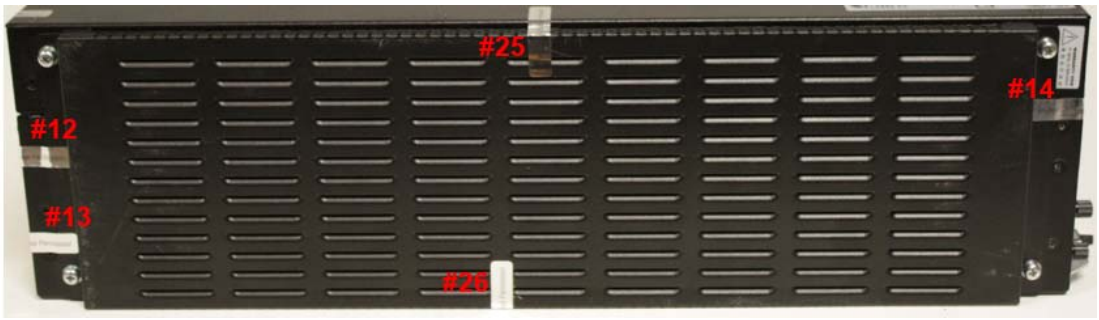

Figure 22: Right Side Plate Seals

Figure 23: Left Side Plate Seals

6.2.3 AR169FGVW-L

The module includes thirteen (13) tamper-evident seals, which are applied to the module as follows:

- Two (2) seals applied to the front, one on each side to prevent undetected removal of the top, baffles, and front cover (see #1 & #2 in Figure 24, Figure 27, and Figure 28)
- One (1) seal applied to the front plate and top (see #3 in Figure 24)
- One (1) seal applied to the front and bottom, preventing port access (see #4 in Figure 24)
- One (1) seal applied to the front plate and bottom (see #5 in Figure 26)
- Two (2) seals applied to the back, one on each side, to prevent undetected removal of the top, baffles, and back cover (see #6 & #7 in Figure 25, Figure 27, and Figure 28)
- One (1) seal applied to the back plate and top (see #8 in Figure 25)
- One (1) seal applied to the back plate and bottom, preventing port access (see #9 in Figure 25 and Figure 26)
- Two (2) seals applied to the right side ventilation cover (see #10 & #11 in Figure 27)
- Two (2) seals applied to the left side ventilation cover (see #12 & #13 in Figure 28)

Figure 24: Front Plate Seals

Figure 25: Back Plate Seals

Figure 26: Bottom and Front Plate Seals

Figure 27: Right Side Plate Seals

Figure 28: Left Side Plate Seals

7 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.

8 Mitigation of Other Attacks Policy

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

9 Security Rules and Guidance

The module design corresponds to the module security rules. The module implements and enforces the following security rules:

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. Zeroization overwrites all CSPs with the “Reset to Factory” service.
5. The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation. When switching between modes, the module zeroizes and forces a reboot before operating in the new mode.

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

6. Upon first time initialization, the Root Administrator (CO) shall authenticate to the module using the default username and password:

   Username: admin
   Password: Admin@huawei
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 update from the default username and password. The minimum password strength is enforced by the module per Section 3.2. The CO can then create Administrator and End User accounts and proceed with module configuration per the vendor provided user manual (available here: http://support.huawei.com/enterprise/en/router/ar3200-pid-6078845).
10. The CO must not configure the failed authentication limit setting for more than 2599.

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