Huawei AC6605
Wireless Access Controller

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.2
Date: June 15, 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	Concurrence Accelerate Platform
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 AC6605 Wireless Access Controller (AC6605) is a multi-chip standalone cryptographic enclosed in hard, commercial grade metal case. The cryptographic boundary for this module is the enclosure. The primary purpose of this module is to handle the configuration of wireless access-points. The module provides network interfaces for data input and output. The module uses FIPS approved algorithms approved by the U.S. government for protecting Unclassified data.

	HW Version & P/N	FW Version
AC6605 Base Model	AC6605-26	V200R007C10SPC100
External Baffles	99089JEB	N/A
Tamper-Evident Seals	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 module is constructed from standard production quality parts. The module is classified as a multi-chip standalone cryptographic module and is enclosed in a hard, commercial grade metal case. The cryptographic boundary for this module is the enclosure. The module is designated as utilizing a non-modifiable operational environment under the FIPS 140-2 definitions. The following diagram shows the major architectural components of the module.

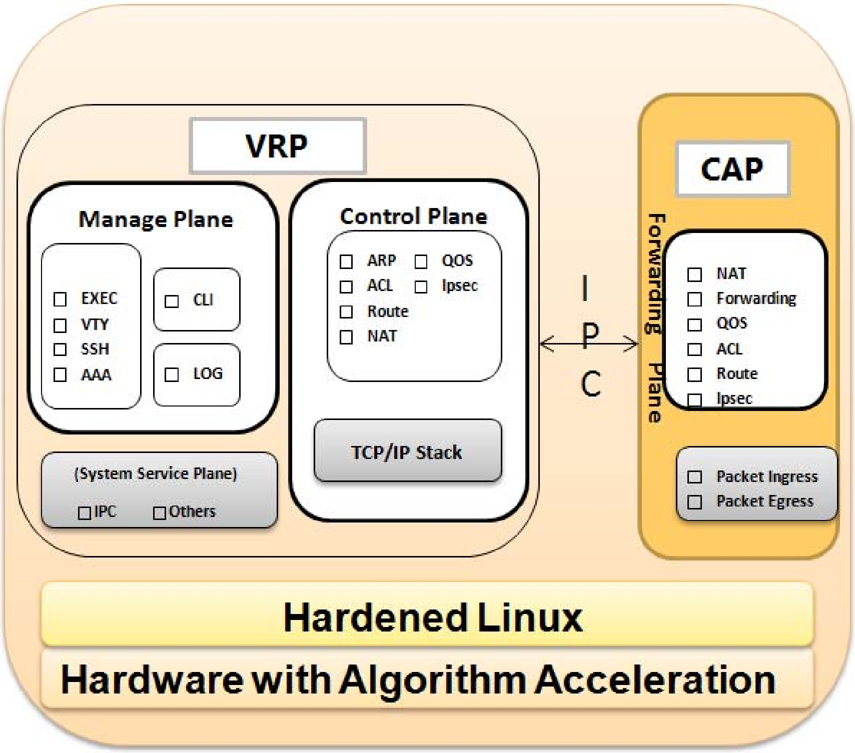
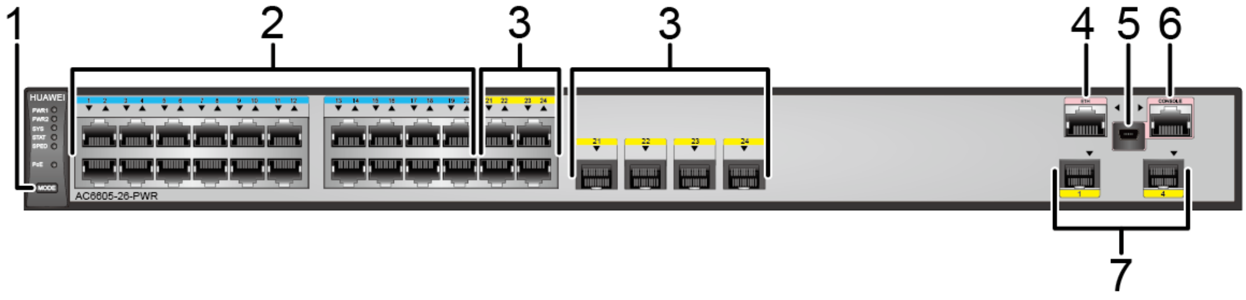


Figure 1 – Access Controller Architectural Block Diagram

1.2 Hardware

The module provides 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. Representations of the module with their ports and interfaces are shown below.

See Section 5.2 for photos with tamper-evident seals and baffles.



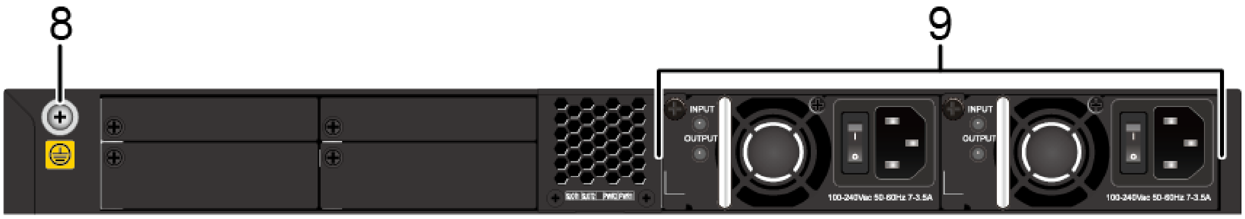


Figure 2 –AC6605 Physical Form

Port	Description	Logical Interface Type
1. MODE	Toggles LED output	Control in
2. BASE-T Net	Network traffic 1-20 (10/100/1000BASE-T)	Control in, Data in, Data out, Status out
3. Combo	Network traffic 21-24 (10/100/1000BASE-T)	Control in, Data in, Data out, Status out
4. Eth Mgmt	Management ethernet connection	Control in, Data in, Data out, Status out
5. Console (Mini USB Connector)	Serial console	Control in, Data in, Data out, Status out
6. Console	Serial console	Control in, Data in, Data out, Status out
7. 10GE SFP+	Network traffic 1-2 (10GE SFP+)	Control in, Data in, Data out, Status out
8. Ground point	Ground point to connect with ground cable.	Power (Ground)
9. Power	Power connector	Power in
LEDs	Power, System, State, Speed, Mode, Service, Console and Ethernet	Status out

Table 5 – AC6605 Ports and Interfaces

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 13 and 14 are available; further, the Establish SSH service is constrained to use only the SSH options listed in Table 6a. In the non-approved mode, all services in Tables 13, 14 and 15 are available for use, and all SSH options from Tables 6a and 6b 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 module are listed in this section.

Table 6a and 6b 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

Table 6a - SSH Security Methods Available in Both modes

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 6b - SSH Security Methods Available in 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 7, Table 8, and Table 9 list all Approved, Allowed and non-Approved algorithms used by the module, respectively.

CAVP	Algorithm	Standard	Mode/Method	Strength[1]	Use
4408	AES	FIPS 197, SP 800-38A	CBC	128[4]	Data Encryption/Decryption
Vendor Affirmed	CKG	SP 800-133	N/A		Key Generation
1114	CVL (SSH[3] KDF)	SP 800-135	SHA-1		KDF used to derive SSH v2 session keys
1421	DRBG[2]	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 HMAC-SHA-256	128 256	Message Authentication
3634	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest Generation

CAVP	Algorithm	Standard	Mode/Method	Strength[1]	Use
2375	Triple-DES	SP 800-67	TCBC	112	Data Encryption/Decryption for IPsec & SSH

Table 7 - Approved Algorithms

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

Algorithm	(Establishment) Strength	Use
Diffie-Hellman (Non SP800-56A compliant)	DH Group 14 (2048-bit modulus) (key agreement; key establishment methodology provides 112 bits of encryption strength)	Key establishment
HMAC-SHA-1-96	Based on HMAC Cert. #2930	Message authentication in SSH
NDRNG	Internal entropy source with rationale to support the claimed DRBG security strength.	DRBG (Cert. #1421) entropy input

Table 8 - 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 (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
HMAC-MD5	For key exchange within SSH, IPsec
IKE (non-compliant)	Key exchange within IPsec
TLS KDF (non-compliant)	Key exchange within TLS
MD5	Message Digest Generation
PBKDF2 (non-compliant)	For 802.11 Master Key derivation
RC4	Element of TLS ciphersuite
RSA (non-compliant)	SSH & TLS key establishment
SM1	Data Encryption/Decryption
SM3	Message Digest Generation
SM4	Data Encryption/Decryption
SNMP KDF (non-compliant)	KDF used to derive SNMP session keys

Table 9 - 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 10 – 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 11 – 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 the console and SSH. The cryptographic module enforces the separation of roles through authenticated connections through standard protocols, programming processes and references. Authentication status does not persist across module power cycles. To change roles, an operator must first log out, then log in using a different role.

Table 12 lists the available roles; the options for authentication type and data are common across roles.

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. Exclusive role for console access.	Identity-based (using *Local password verification*)	Username and Password
Administrative User (AU)	Configures and administers the module per the delegated access rights assigned by the Root Administrator.		

Table 12 – Roles Description

3.2 Authentication Methods

The *Local password verification* method 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).

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 seven (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 one in 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.

Boot menu authentication through the console will powercycle the module after three (3) unsuccesful attempts. The module takes over three (3) minutes to powercycle, thus only three (3) authentication attempts are possible in a one minute period.

The probability of a false authentication in a one minute period is 3/(2.6x10^8), which is less than 1 in 100,000.

Normal console authentication, requires a waiting period of five (5) seconds after each failed 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.

3.3 Services

All services implemented by the module are summarized next, with additional detail provided in

Service	Description	CO	AU
Configure System	License management, file management, and logging configuration.	X	
Configure Network	Network Interface configuration and management.	X	X[2]
Module Reset	Reboot the module via reset CLI command. This service executes the suite of self-tests required by FIPS 140-2.	X	X[2]
Status Monitoring and Reporting	Provides module status (CPU usage, etc.) and logs.	X	X[2]
User Management and Authentication	Creating users and setting access rights.	X	X[2]
Reset to Factory	This restores the module to factory defaults and is the means of providing zeroization of some CSPs	X	X[2]

Table 13 – Authenticated Module Services

[2] Administrative user's service access level (0-15) is set by the CO. Only a user level between 3 and 15 can manage other administrative accounts.

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 Table 6 may be used. In the non-Approved mode, all methods in Tables 6 and 7 may be used.
Network Traffic	Provides network services through WAN, Uni/Multicast routing, QoS, Ethernet switching, IP services (DHCP, DNS, NAT).
Show Status	This service provides the current status of the cryptographic module indicators on the device show the module running properly or restarting.

Table 14 – Unauthenticated Module Services

Service	Description
BGP and BGP4+	Routing protocol
CAPWAP	Control And Provisioning of Wireless Access Points Protocol Specification
Configure Policy	Configure VPN access policy
Ftp	File Transfer Protocol
HTTP	Web interface for configuration.
ISIS and ISISv6	Routing protocol
L2TP	Functioning as the LAC or LNS and allowing concurrent user access on multiple channels
NTP	Time synchronization for traditional IP networks
OSPFv2 and OSPFv3	Routing protocol
Remote AAA	Connection to remote AAA server (RADIUS, TACACS)
RIP and RIPng	Routing protocol
SNMP	Configuration, administration and monitoring
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
VPN	Virtual Private Network through IPsec
VRRP	Redundancy backup mechanism for IP services, including IPv4/IPv6 VRRP

Table 15 –Services only available in Non-Approved mode

The next table describes 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	--	--	--	--	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--
Root Administrator (CO)									
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
Reset to Factory	WZ	Z	Z	--	--	Z	Z	--	Z
Status Monitoring and Reporting	RE	--	--	--	--	--	--	--	--
User Management and Authentication	RWEZ	--	--	--	--	--	--	--	--
Administrative User (AU)									
Configure Network	RE	GE	GE	--	GWZ	--	--	GWZ	--
Module Reset	--	Z	Z	Z	--	Z	Z	--	Z
Reset to Factory	WZ	Z	Z	Z	--	Z	Z	--	Z
Status Monitoring and Reporting	--	--	--	--	--	--	--	--	--
User Management and Authentication	RWEZ	--	--	--	--	--	--	--	--

Table 16 – 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 17 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 module's SYS_LED will go from quick flash in green at 4Hz to slow flash in green at 0.5Hz. If a failure of a self-test occurs, the module enters an error state, the module SYS_LED will keep quick flash in green, outputs the following error message on the console and forces the module to reboot: "Self-Test Fail…".

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[3]
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
HMAC (#2930)	Separate HMAC generation and verification KATs, using SHA-1 Separate HMAC generation and verification KATs, using SHA-256
ECDSA (#1060)	Pairwise consistency test
SHS (#3634)	Separate KAT of SHA-1 and SHA-512 (SHA-256 tested in HMAC KAT)

Table 17 – 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 18 – Conditional Self-tests

[3] Even though the module does not use key sizes of 192 and 256 bit in an approved mode, they are still tested.

5 Physical Security Policy

The cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper-evident material and tamper-evident seals
- Protected vents

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 seals based on the schedule described in Table 19 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.
External Baffles	Inspect monthly

Table 19 – Physical Security Inspection Guidelines

5.1 External Baffle Installation

The AC6605 has three (3) external baffles that provide opacity to the module vent openings and needs to be installed prior to tamper seal application.

NOTE

After the CO applies the opaque enclosures, the operational temperature range of the AC6005 will be -5°C to +50°C.

5.2 Tamper Seal Placement

The CO should ensure the module enclosure surface is clean and dry prior to the application of seals. The module contains seventeen (17) tamper-evident seals, which are applied to the module as follows:

Figure 3 and Figure 4 show the installation locations of AC6605 tamper seals.

- [1] [2] [15] [16] Cover both the filler panel and the top of the chassis.
- [11] [12] [13] [14] Cover both the filler panel and bottom of chassis.
- [3]: Cover both the filler panel and the top of the chassis.
- [4]: Cover both the power module and the bottom of the chassis.
- [5]: Cover both the fan panel and the top of the chassis.
- [17]:Cover both the fan and the power module of the chassis.
- [6] [8]: Cover both the filler panel and the bottom of the chassis.
- [7] [9]: Cover both the filler panel and the top of the chassis.
- [10]: Cover both the rear and right of the chassis.

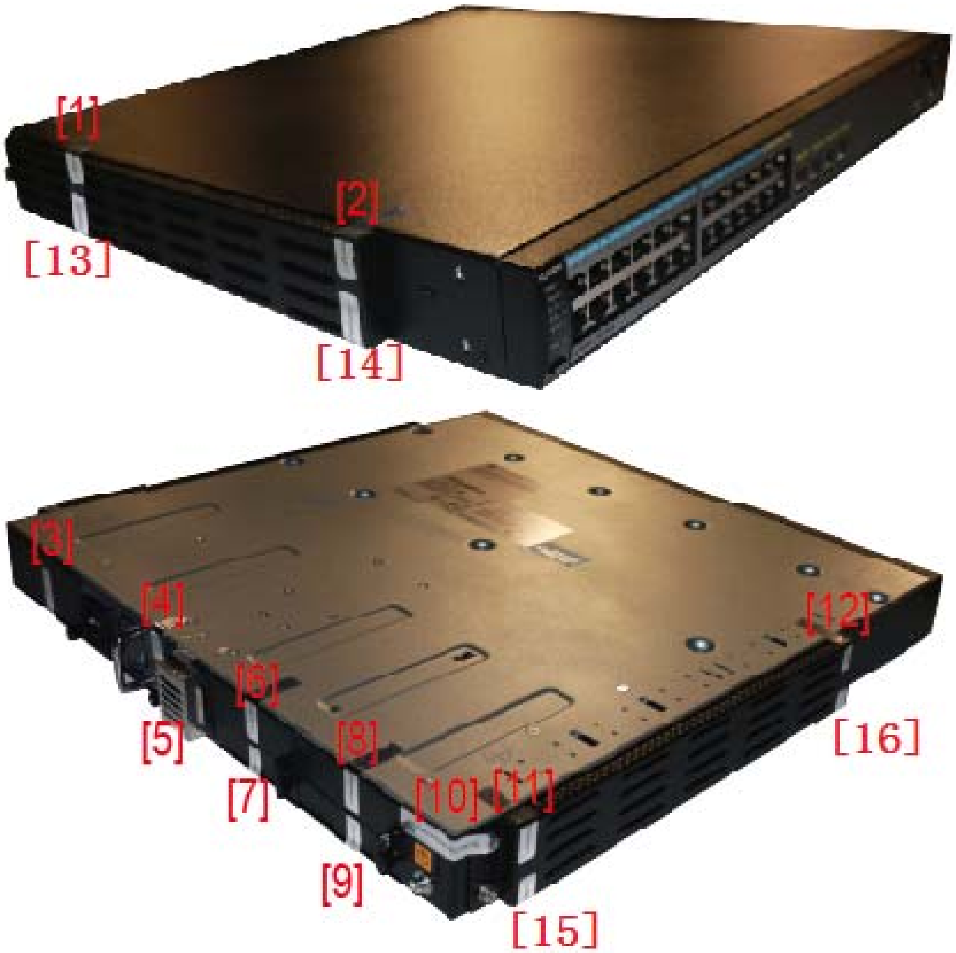


Figure 3 - AC6605 Tamper-evident Seal Placement

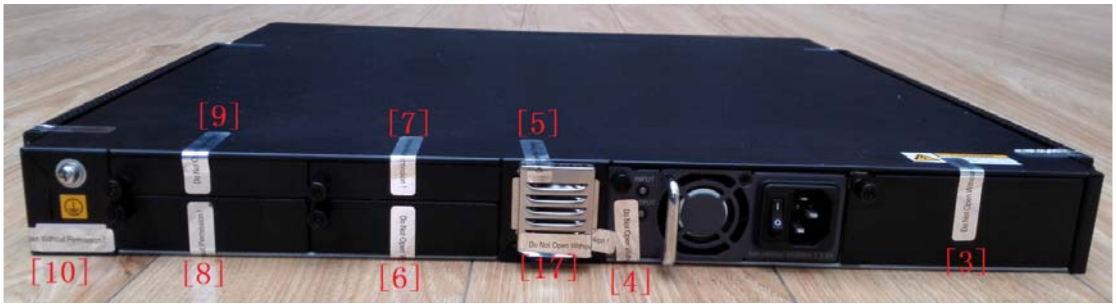


Figure 4 - AC6605 Tamper-evident Seal Placement

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

8 Security Rules and Guidance

The module design 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. The operator shall remain in control of the module until the zeroization process completes Zeroization overwrites all CSPs and is performed with the following procedure:
   - Reset the boot menu password using the "reset boot password" command.
   - Zeroize the ECC key pair using the "ecc local-key-pair destroy" command.
   - Delete previous saved configurations using the “reset saved-configuration” 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 Root Administrator (CO) 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 username and password for the following: boot menu admin, console admin, SSH admin. The minimum password strength is enforced by the module per Section 3.2. The CO can then create additional Administrative User accounts and proceed with module configuration per the vendor provided Configuration Guide (available here: http://support.huawei.com/enterprise/en/wlan/ac6605-pid-7974000).
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.