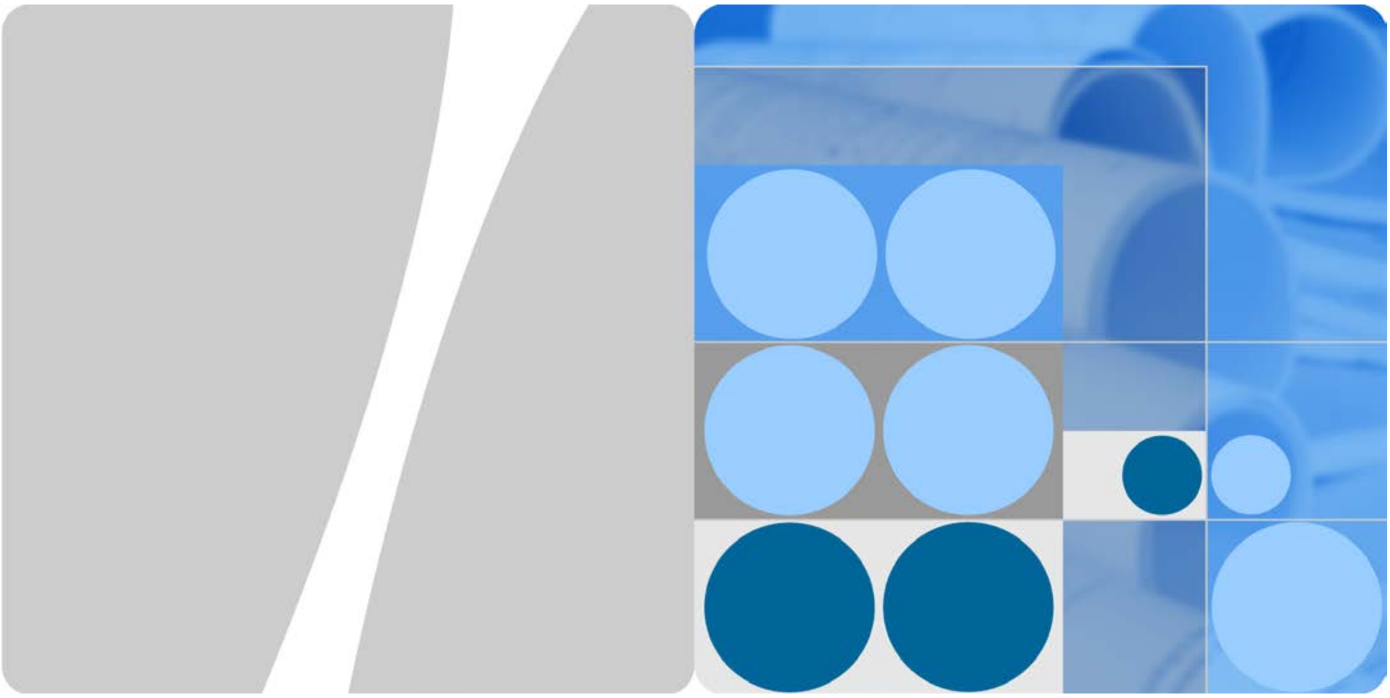


Huawei USG 6000 Series Firewall

Non-Proprietary Security Policy

Issue	03
Date	2017-09-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Purpose

This document describes the Security Policy of the Huawei USG 6000 Series Firewall consisting of the USG6310S/6370/6620/6650/6680.

Intended Audience

This document is intended for administrators who configure and manage the USG6310S/6370/6620/6650/6680. The administrators must have good Ethernet knowledge and network management experience.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠ NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
🕮 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Date	Description
01	2017 05 19	This issue is the first official release.
02	2017 09 22	Updates per CMVP comments

Contents

1 References and Definitions

Table 1-1 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 1-2 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
AAPT	Anti-APT feature
CLK	Clock

Term	Definition
ESP	Encapsulated Security Payload (a subset of IPsec, Internet Protocol Security)
IKE	Internet Key Agreement, a key agreement scheme associated with IPsec (but not used by the module)
GUI	Graphical User Interface
IETF	Internet Engineering Task Force, a standards body
IPS	Intrusion Prevention System
KPM	Key-Pair Management
KX	Key Exchange
LDAP	Lightweight Directory Access Protocol
MPLS	Multiprotocol Label Switching
NTP	Network Time Protocol
OSPF	Open Shortest Path First
RFC	Request For Comment; the prefix used by IETF for internet specifications.
RIP	Routing Information Protocol
SSH	Secure Shell
VPN	Virtual Private Network
TLS	Transport Layer Security
TOD	Time of Day
TSM	Terminal Security Management
UDP	User Datagram Protocol
WSIC	Wide Service Interface Card

2 Introduction

Huawei USG 6000 Series Firewall consisting of HUAWEI USG6310S/6370/6620/6650/6680 models 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 provide secure remote access to internal resources via the Internet Protocol (IP). 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 limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

Table 2-1 Cryptographic module configurations

No.	Module	HW P/N and Version	FW Version
1	USG6310S	50050064 Rev. G	V500R001C50
2	USG6370	0235G7LL Rev. P.4	V500R001C50
3	USG6620	02359519 Rev. G.3	V500R001C50
4	USG6650	0235G7G4 Rev. U.3	V500R001C50
5	USG6680	0235G7G7 Rev. U.2	V500R001C50

Table 2-2 External baffle and tamper seal

Module	Number	Version
External Baffle	99089JEB	A.2
Tamper seal	4057-113016	A.3

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

Table 2-3 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

2.1 Hardware

The physical forms of each configuration of the module are depicted in Figure 2-2 through Figure 2-6 with corresponding ports and interfaces in Table 2-4 through Table 2-8.

Figure 2-2 USG6310S physical form

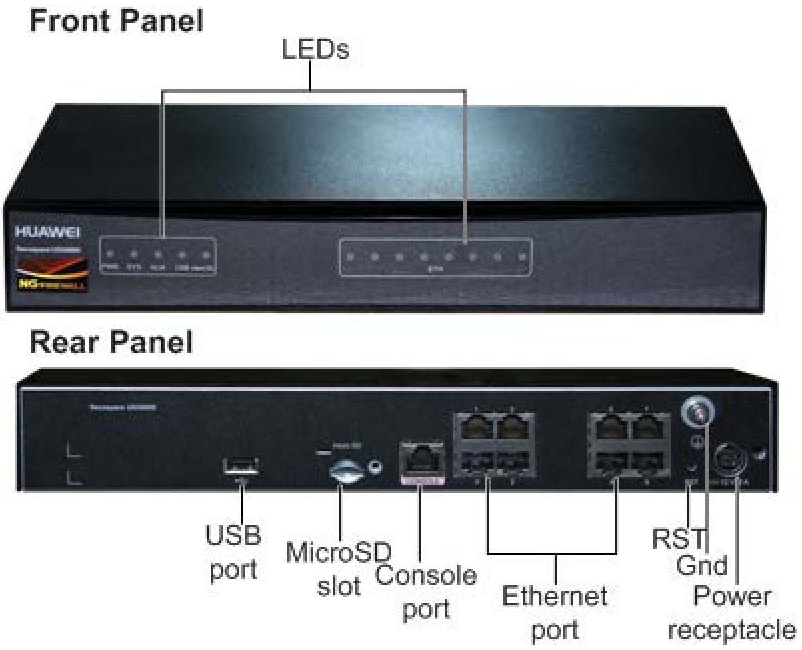


Table 2-4 USG6310S ports and interfaces

Port	Description	Logical Interface Type
Console	Serial console	Control in, Data in, Data out, Status out
Ethernet	Network traffic connections (8)	Control in, Data in, Data out, Status out
LEDs	Power, System, Alarm, USB, microSD and Ethernet (8)	Status out
MicroSD	MicroSD memory card slot	N/A - Covered with tamper seal
Power and Gnd	DC power	Power
RST	Reset button	Control in
USB	USB interface	N/A - Covered with tamper seal

Figure 2-3 USG6370 physical form

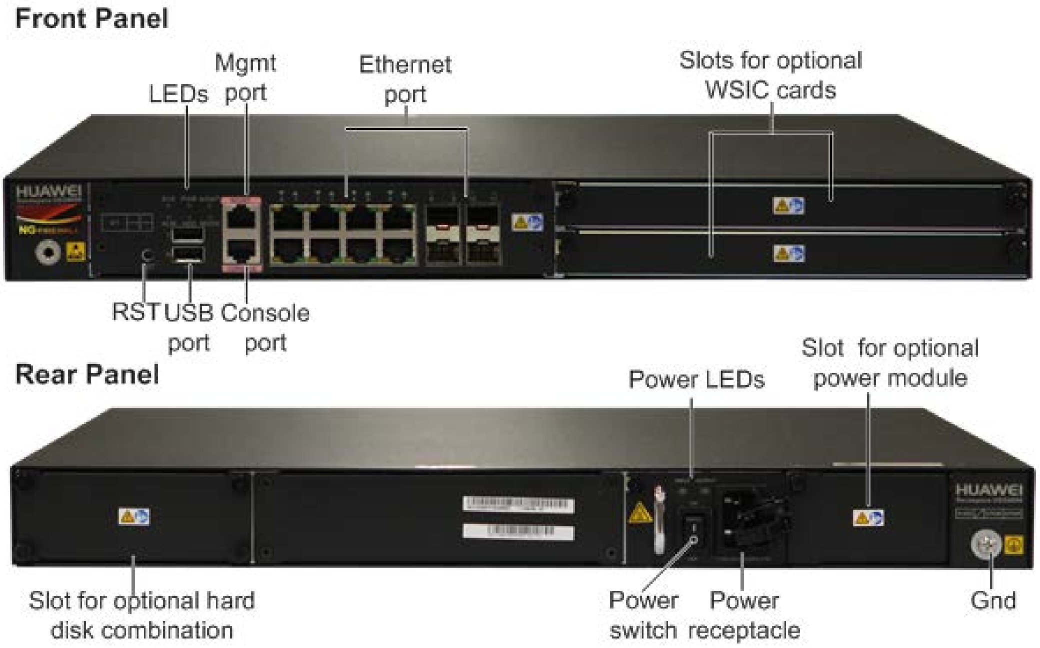


Table 2-5 USG6370 ports and interfaces

Port	Description	Logical Interface Type
Console	Serial console	Control in, Data in, Data out, Status out
Ethernet	Network traffic connections (12)	Control in, Data in, Data out, Status out
WSIC slots	Optional WSIC card slots (2)	Control in, Data in, Data out, Status out
LEDs	System, Alarm, Mode, HDD, Mgmt, Power (3)	Status out
Mgmt	Management Ethernet connection	Control in, Data in, Data out, Status out
Power and Gnd	AC power with switch (2)	Power
RST	Reset button	Control in
USB	USB interface (2)	N/A - Covered with tamper seal
HDD slot	Optional Dard Disk slot	Data in, Data out, Status out

Figure 2-4 USG6620 physical form

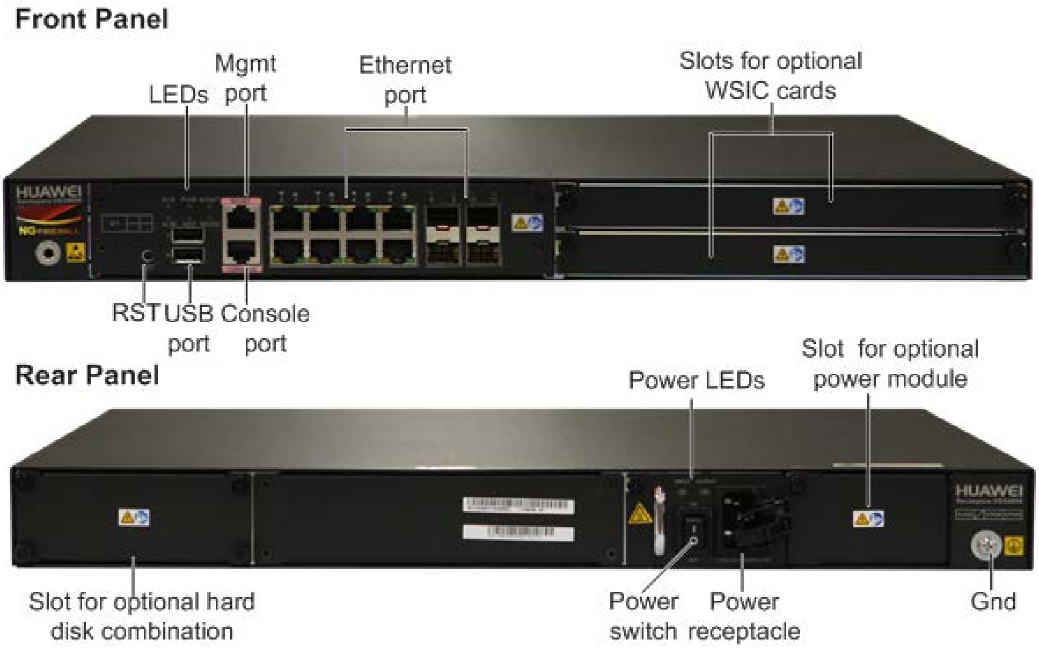


Table 2-6 USG6620 ports and interfaces

Port	Description	Logical Interface Type
Console	Serial console	Control in, Data in, Data out, Status out
Ethernet	Network traffic connections (12)	Control in, Data in, Data out, Status out
WSIC slots	Optional WSIC card slots (2)	Control in, Data in, Data out, Status out
LEDs	System, Alarm, Mode, HDD, Mgmt, Power (3)	Status out
Mgmt	Management Ethernet connection	Control in, Data in, Data out, Status out
Power and Gnd	AC power with switch (2)	Power
RST	Reset button	Control in
USB	USB interface (2)	N/A - Covered with tamper seal
HDD slot	Optional Dard Disk slot	Data in, Data out, Status out

Figure 2-5 USG6650 physical form

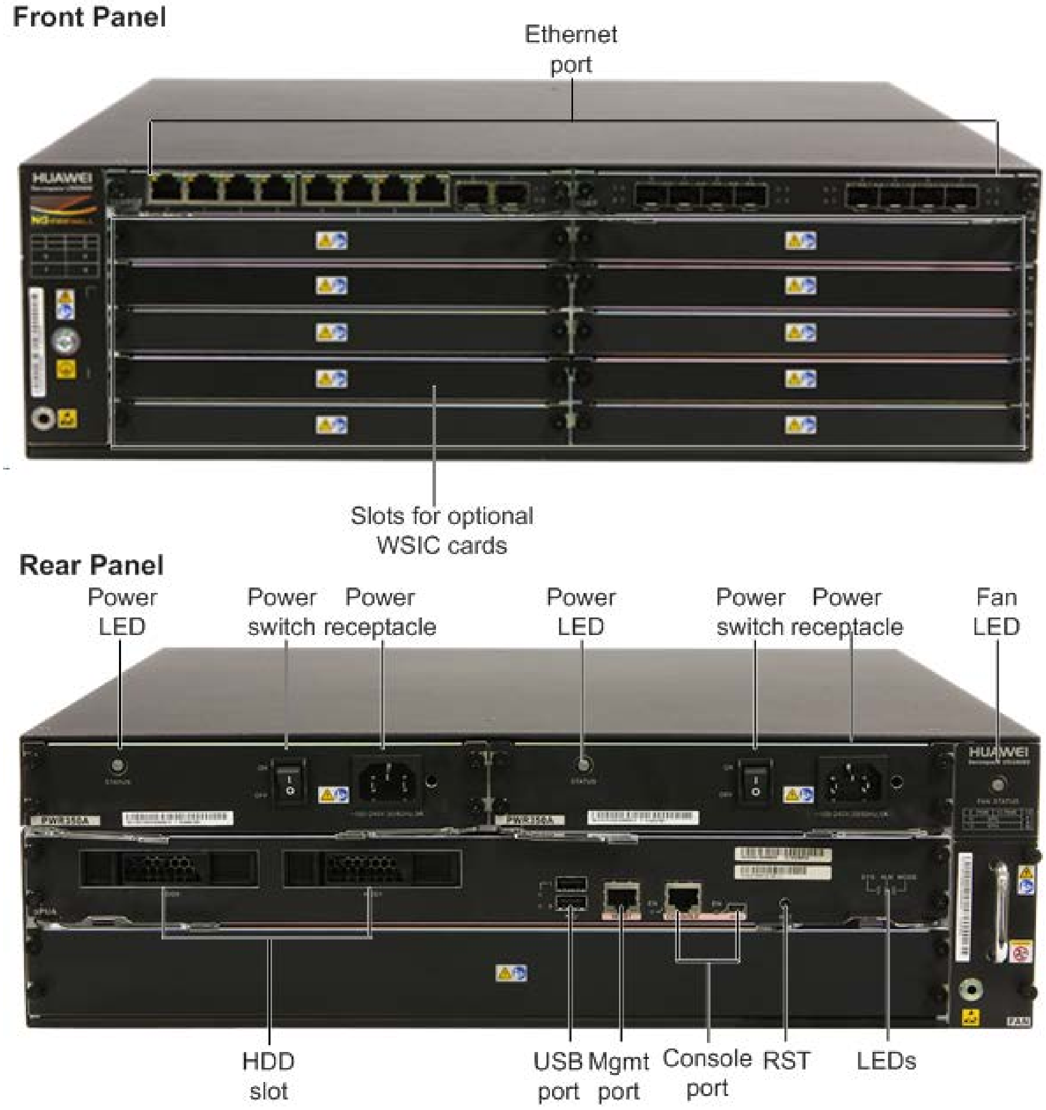


Table 2-7 USG6650 ports and interfaces

Port	Description	Logical Interface Type
Console	Serial console or mini USB serial	Control in, Data in, Data out, Status out
Ethernet	Network traffic connections (18)	Control in, Data in, Data out, Status out
WSIC slots	Optional WSIC card slots (10)	Control in, Data in, Data out, Status out
LEDs	System, Alarm, Mode, Fan, Console (2), USB (2), Power (2)	Status out
Mgmt	Management Ethernet connection	Control in, Data in, Data

Port	Description	Logical Interface Type
		out, Status out
Power	Two AC power inputs with switches	Power
RST	Reset button	Control in
USB	Two USB interfaces	N/A - Covered with tamper seal
HDD slots	Optional Dard Disk slot (2)	Data in, Data out, Status out

Figure 2-6 USG6680 physical form

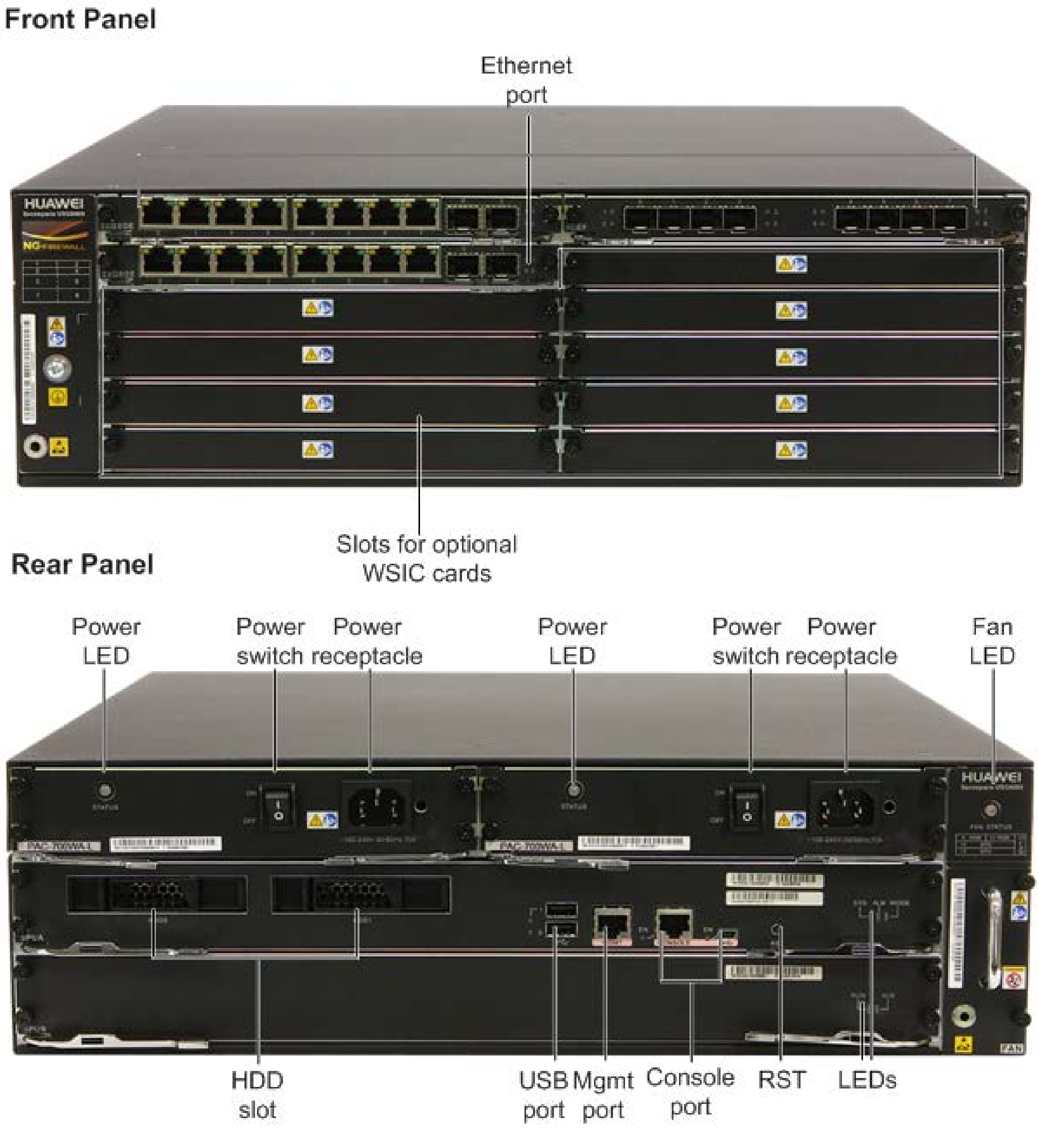


Table 2-8 USG6680 ports and interfaces

Port	Description	Logical Interface Type
Console	Serial console or mini USB serial	Control in, Data in, Data out, Status out
Ethernet	Network traffic connections (28)	Control in, Data in, Data out, Status out
WSIC slots	Optional WSIC card slots (9)	Control in, Data in, Data out, Status out
LEDs	System, Alarm (2), Mode, Fan, Console (2), USB (2), Run, Power (2)	Status out
Mgmt	Management Ethernet connection	Control in, Data in, Data out, Status out
Power	Two AC power inputs with switches	Power
RST	Reset button	Control in
USB	Two USB interfaces	N/A - Covered with tamper seal
HDD slots	Optional Dard Disk slot (2)	Data in, Data out, Status out

2.2 Exclusion

USG6370 and USG6620

The USG6370 and USG6620 models support the following optional components:

- Wide Service Interface Cards (WSIC): installed in the expansion slots to provide additional throughput.
- Hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B: Hard disks are used to store logs and reports, and they can be purchased from Huawei if necessary.

These components are not involved in any security-related service. These components do not process any keys or CSPs.

Table 2-9 WSIC cards

WSIC	Top P/N Rev
8GE	0302G3A4 Rev. H.4
2XG8GE	0302G3C9 Rev. H.5
8GEF	0302G3AC Rev. H.5
4GE-BYPASS	0302G3A7 Rev H.3

Table 2-10 Hard disks

Hard Disk	Top P/N Rev
Hard Disk Combination SM-HDD-SAS300G-B	02358140 Rev. F.3
Hard Disk Combination SM-HDD-SAS600G-B	02350YBC Rev. D.3
Hard Disk Combination SM-HDD-SAS1200G-B	02351CRD Rev. C.3

Figure 2-7 8GE card panel

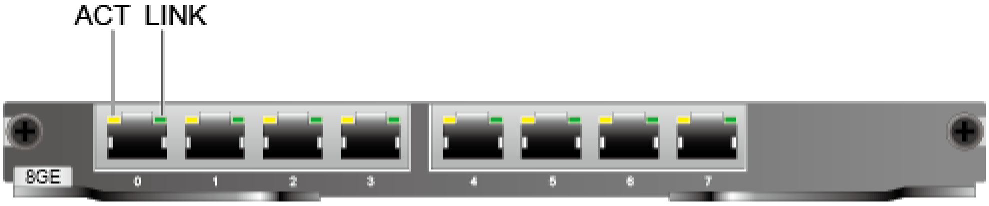


Table 2-11 8GE card ports and interfaces

Port	Description	Logical Interface Type
LEDs	Link, ACT	Status out
Ethernet	Network traffic connections (8)	Control in, Data in, Data out, Status out

Figure 2-8 2XG8GE card panel

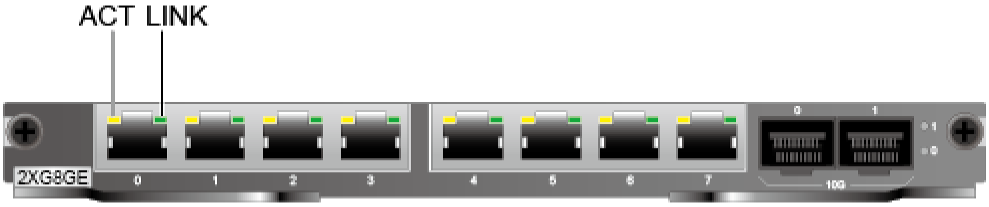


Table 2-12 2XG8GE card ports and interfaces

Port	Description	Logical Interface Type
LEDs	Link, ACT, SFP+ 0, SFP+ 1	Status out
Ethernet	Network traffic connections (10)	Control in, Data in, Data out,

Port	Description	Logical Interface Type
		Status out

Figure 2-9 8GEF card panel

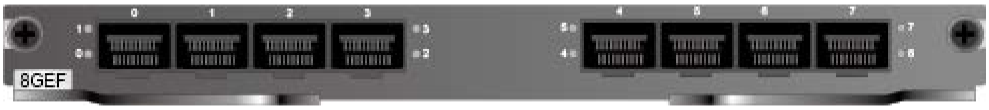


Table 2-13 8GEF card ports and interfaces

Port	Description	Logical Interface Type
LEDs	SFP+ 0 - 4	Status out
Ethernet	Network traffic connections (8)	Control in, Data in, Data out, Status out

Figure 2-10 4GE-BYPASS card panel

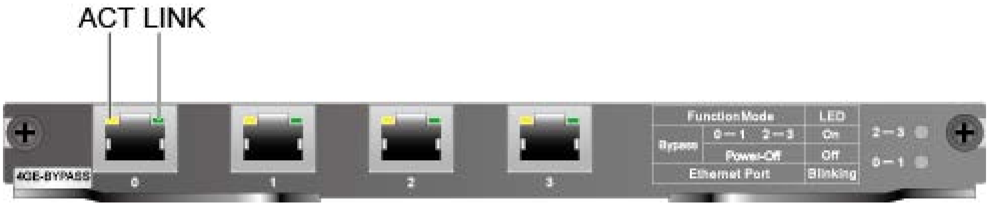


Table 2-14 4GE-BYPASS card ports and interfaces

Port	Description	Logical Interface Type
Ethernet	Network traffic connections (4)	Control in, Data in, Data out, Status out

The physical appearance of the hard disk combination SM-HDD-SAS300G-B/SM-HDD-SAS600G-B/SM-HDD-SAS1200G-B is identical. The following uses the SM-HDD-SAS300G-B as an example.

Figure 2-11 Appearance of the hard disk combination SM-HDD-SAS300G-B

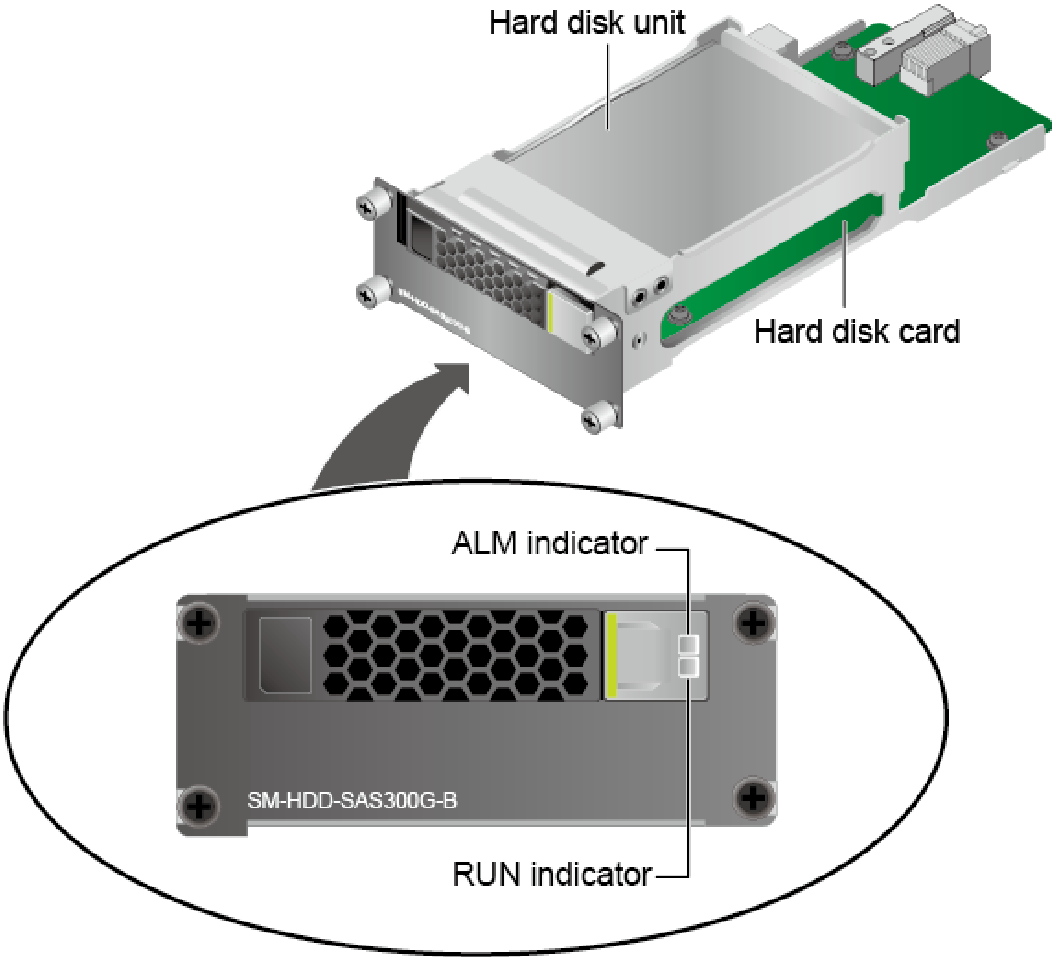


Table 2-15 SM-HDD-SAS300G-B ports and interfaces

Port	Description	Logical Interface Type
LEDs	RUN, ALM	Status out

USG6650 and USG6680

The USG6650 and USG6680 models support the following optional components:

- WSIC cards: installed in the expansion slots to provide more ports or functions.
- Hard disk unit SM-HDD-SAS300G-A, SM-HDD-SAS600G-A or SM-HDD-SAS1200G-A: Hard disks are used to store logs and reports. You can purchase one or two hard disks from Huawei if needed. To ensure hard disk data reliability, you are advised to purchase two hard disks with the same capacity to create RAID1 for data backup.

These components are not involved in any security-related service. These components do not process any keys or CSPs.

Table 2-16 WSIC cards

WSIC	Top P/N Rev
8GE	0302G3A4 Rev. H.4
2XG8GE	0302G3C9 Rev. H.5
8GEF	0302G3AC Rev. H.5
4GE-BYPASS	0302G3A7 Rev. H.3

Table 2-17 Hard disks

Hard Disk	Top P/N Rev
Hard Disk Combination SM-HDD-SAS300G-A	0235G7GC Rev. K.4
Hard Disk Combination SM-HDD-SAS600G-A	02350QLB Rev. C.4
Hard Disk Combination SM-HDD-SAS1200G-A	02351CQQ Rev. A.6

The physical appearance of the hard disk units, SM-HDD-SAS300G-A/SM-HDD-SAS600G-A/SM-HDD-SAS1200G-A, is identical. The following uses the SM-HDD-SAS300G-A as an example.

Figure 2-12 Appearance of the hard disk unit SM-HDD-SAS300G-A

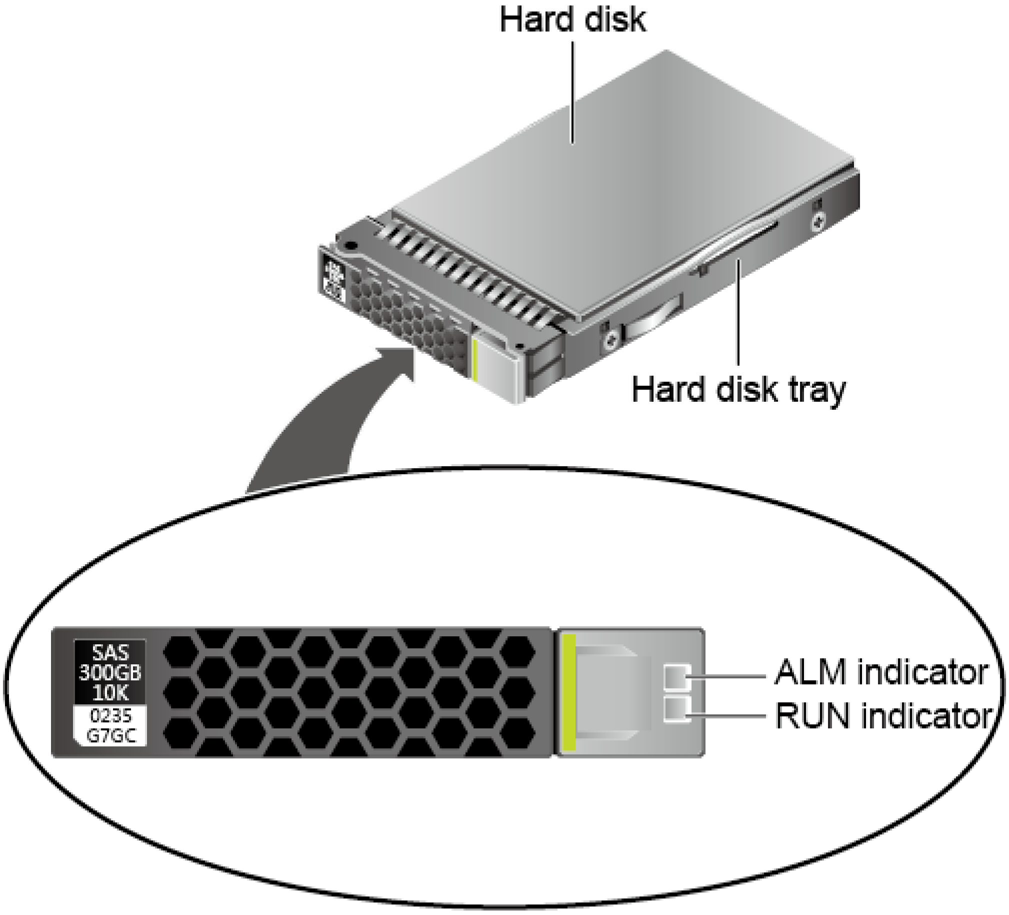


Table 2-18 SM-HDD-SAS300G-B ports and interfaces

Port	Description	Logical Interface Type
LEDs	RUN, ALM	Status out

2.3 Modes of Operation

The module supports both Approved and non-Approved modes of operation. By default, the module comes configured in the non-Approved mode. In the non-Approved mode, the additional ciphersuites shown in Table 3-2 are available. In addition, SSH v1.5 and SNMP v1/2 are available for configuration, administration and monitoring.

See 9 Security Rules and Guidance for additional Approved mode operation guidance.

3 Cryptographic Functionality

The cryptographic protocols and primitives implemented and used by the modules are listed in this section. Tables 3-1 and 3-2 list the TLS ciphersuites available in the Approved and non-Approved modes, respectively. Table 3-3 lists the SSH security methods; unlike TLS ciphersuites, SSH methods are independently selectable and may be used in any combination. Table 3-4 lists the IPsec security methods.

The module supports HTTPS using TLS ciphersuites below in the Approved mode, supporting STS to redirect all HTTP connections to HTTPS (with TLS) and to assure that a user cannot accidentally downgrade browser security.

Table 3-1 TLS ciphersuites used in the Approved mode

Cipher Suite String(IETF enumeration)	TLS	KX	Cipher	Digest
TLS1_CK_RSA_WITH_AES_256_SHA	1.1, 1.2	RSA	AES-256	SHA-1 SHA-2
TLS1_CK_RSA_WITH_AES_128_SHA	1.1, 1.2	RSA	AES-128	SHA-2
TLS1_CK_DHE_RSA_WITH_AES_256_SHA	1.1, 1.2	DH	AES-256	SHA
TLS1_CK_DHE_RSA_WITH_AES_128_SHA	1.1, 1.2	DH	AES-128	SHA
TLS12_CK_RSA_AES_256_CBC_SHA256	1.2	RSA	AES-256	SHA-2

Table 3-2 TLS ciphersuites used in the non-Approved mode

Cipher Suite String (OpenSSL Enumeration)	TLS	KX	Cipher	Digest
TLS_RSA_WITH_DES_CBC_SHA	1.0, 1.1, 1.2	RSA	DES	SHA-1
TLS_RSA_WITH_RC4_128_MD5	1.2	RSA	RC4	MD5
TLS_RSA_WITH_RC4_128_SHA	1.2	RSA	RC4	SHA-1
TLS_RSA_WITH_NULL_MD5	1.0	RSA	NULL	MD5
TLS_RSA_WITH_NULL_SHA	1.0	RSA	NULL	SHA-1

Cipher Suite String (OpenSSL Enumeration)	TLS	KX	Cipher	Digest
TLS_DHE_RSA_WITH_DES_CBC_SHA	1.2	DH	DES	SHA-1
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	1.2	DH (2048)	Triple-DES	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	1.2	DH (2048)	AES-128	SHA-256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	1.0, 1.1, 1.2	DH (2048)	AES-256	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	1.2	DH	AES-256	SHA-256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	1.0, 1.1, 1.2	DH	AES-256	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	1.2	DH	AES-128	SHA-256
TLS1_CK_RSA_RC4_128_SHA	1.1,1.2	RSA	AES-256	SHA-1

The module uses SSHv2 over a shell interface via the console serial port to perform limited module configuration and administration.

Table 3-3 Available SSH security methods

SSH Security Methods	Approved Mode	Non-Approved Mode
Key Exchange		
diffie-hellman-group-exchange-sha1	X	X
diffie-hellman-group14-sha1	X	X
diffie-hellman-group1-sha1		X
Server Host Key (Authentication)		
ssh-dsa		X
ssh-rsa	X	X
ssh-ecdsa	X	X
Digest		
hmac-sha2-256	X	X
hmac-md5-96		X
hmac-md5		X

SSH Security Methods	Approved Mode	Non-Approved Mode
hmac-sha1	X	X
hmac-sha2-256-96	X	X
hmac-sha1-96	X	X
Cipher		
DES_CBC		X
Triple-DES	X	X
AES128_CBC	X	X
AES128_CTR	X	X
AES256_CBC	X	X
AES256_CTR	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 or GCM mode with IKE v1/v2 key exchange. GCM IV constructed per IG A.5 scenario 2.

Table 3-4 Available IPsec ESP cipher and digest methods

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
AES128-GCM	AES-128	GMAC
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
AES256-GCM	AES-256	GMAC
AES192-CBC-SHA	AES-192	SHA-1
AES192-CBC-SHA256	AES-192	SHA-256
AES192-CBC-SHA384	AES-192	SHA-384

Cipher Suite String (IETF Enumeration)	Cipher	Digest
AES192-CBC-SHA512	AES-192	SHA-512
AES192-GCM	AES-192	GCM
3DES-CBC-SHA	3DES	SHA-1
3DES-CBC-SHA256	3DES	SHA-256
3DES-CBC-SHA384	3DES	SHA-384
3DES-CBC-SHA512	3DES	SHA-512

The module uses SNMP (exclusively using AES and HMAC-SHA cryptography as defined in RFC2574, RFC 3414 and RFC 3826 SNMP extension specifications) for module configuration reporting and status monitoring only.

Table 3-5, Table 3-6 and Table 3-7 list all Approved, Allowed and non-Approved algorithms used by the library, respectively.

Table 3-5 Approved algorithms

CAVP	Algorithm	Standard	Mode/Method	Strength[1]	Use
Library: VPP					
4451	AES	FIPS 197, SP 800-38A	CBC, CFB	128, 192,256	Data Encryption/Decryption
4451/ 2393 2954	AES/Triple-DES HMAC	SP800-38F	Key Wrap	128,192, 256	Key Establishment
Vendor Affirmed	CKG	SP 800-133	N/A		Key Generation
1152	CVL SNMP KDF[3]	SP800-135	SHA-1		KDF used to derive SNMP AES and HMAC keys
	CVL SSH KDF	SP800-135	SHA-1		KDF used to derive SSH v2 session keys
	CVL TLS KDF	SP800-135	SHA-256, 384, 512		Tested but not used by the module
1153	CVL ECC CDH	SP 800-56A	P-256 P-384 P-521		Shared key calculation
1442	DRBG[2]	SP 800-90A	CTR_DRBG	256	Deterministic Random Bit

CAVP	Algorithm	Standard	Mode/Method	Strength[1]	Use
					Generation
1084	ECDSA	FIPS186-4	P-256 SHA-256 P-384 SHA-384 P-521 SHA-512 P-256 P-384 P-521 P-256 SHA-256 P-384 SHA-384 P-521 SHA-512		Signature Generation Key Pair Generation Signature Verification
2954	HMAC	FIPS 198-1 IG A.8	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 HMAC-SHA-1-96	128 192 256	Message Authentication
2432	RSA	FIPS 186-2 FIPS186-4	Mod 2048,3072 Mod 2048,3072,4096 (SHA-1/256/384/512) Sig. Gen w/SHA-1 for protocol use only Mod 1024,2048,3072,4096 (SHA-1/256/384/512)		RSA Key Generation Signature Generation Signature Verification
3664	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384,SHA-512		Message Digest Generation
2393	Triple-DES	SP 800-67	TCBC 3-Key		Data Encryption/Decryption
Library: OpenSSL					
4449	AES	FIPS 197, SP 800-38A	CBC, GCM	128, 192,256	Data Encryption/Decryption
1148	CVL TLS[3] KDF	SP800-135	TLS 1.0/1.1/1.2 (SHA-256) (SHA-384/512 tested but not used)		KDF used to derive TLS session keys
	CVL IKE KDF	SP800-135	IKEv1/2: 2048 (SHA-1, 256, 384, 512)		KDF used to derive IKE v1/v2 session keys
1149	CVL	SP 800-56A	P-256 P-384 P-521		Shared key

CAVP	Algorithm	Standard	Mode/Method	Strength[1]	Use
	ECC CDH				calculation
1440	DRBG[2]	SP 800-90A	CTR_DRBG 256		Deterministic Random Bit Generation
2952	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	128 192 256	Message Authentication
2430	RSA	FIPS 186-4	Mod 2048,3072 Mod 2048,3072,4096 (SHA-1/256/384/512) Sig. Gen w/SHA-1 for protocol use only Mod 1024,2048.3072,4096 (SHA-1/256/384/512)		RSA Key Generation Signature Generation Signature Verification
3662	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384,SHA-512		Message Digest Generation
2391	Triple-DES	SP 800-67	TCBC	3-Key	Data Encryption/Decryption

Table 3-6 Allowed algorithms

Algorithm	(Establishment) Strength	Use
Diffie-Hellman	(CVL Certs. #1148 and #1152) Provides 112, 128 or 256 bits of encryption strength.	Key establishment.
EC Diffie-Hellman	(CVL Certs. #1149 and #1153) Provides 112, 128 or 256 bits of encryption strength	Key establishment
MD5	No strength claimed.	TLS 1.0/1.1 KDF
NDRNG	Internal entropy source with rationale to support the claimed DRBG security strength.	DRBG (Certs. #1440, #1441, #1442) entropy input.
RSA Key Wrapping	Provides 112 or 128 bits of encryption strength.	Key establishment.

[1] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli

[2] Prediction resistance; block_cipher_df used for instantiation.

[3] No parts of the TLS, SSH, and SNMP protocols, other than the KDF, have been reviewed or tested by the CAVP

Table 3-7 Non-Approved algorithms (used only in the non-Approved mode)

Algorithm	Use
DES	Encryption/Decryption in SSL VPN and IPsec.
DH Group 1	For key exchange within SSH, IPSec.
DH Group 2	For key exchange within IPSec.
DH Group 5	For key exchange within IPSec.
DSA (non-compliant)	For use within SSH.
HMAC-MD5	For use within SSH.
MD5	Hashing of non-security relevant data.
RC4	Element of the TLS ciphersuite allowed only in non-Approved mode.
RSA	512-bit or 1024-bit key sizes for Signature generation.
SM2	Create key pair.
Triple-DES (Two-key)	Encryption/Decryption that provides only 80 bits of security.

3.1 Critical Security Parameters and Public Keys

All Critical Security Parameters (CSPs) used by the module are described in this section. Symmetric keys generated internally to the module are the result of unmodified output from the DRBG.

Table 3-8 CSPs

Name	Description and Use
DRBG-SEED	Seed material used to seed or reseed the DRBG; entropy input to the block_cipher_df used to instantiate the Approved CTR_DRBG.
DRBG-STATE	SP 800-90A CTR_DRBG V and Key values (AES-256 Key, 128-bit V, per IG 14.5).
IPSec-SENC	ESP Session Encryption key. AES-128, AES-192, AES-256 or 3DES key for IPsec ESP tunnel message encryption/decryption.
IPSec-SMAC	ESP Session Authentication Key. HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 or HMAC-SHA2-512 for IPSec ESP tunnel message authentication.
IKE-DH-PRIV	IKE ephemeral Diffie-Hellman private key for key exchange.

Name	Description and Use
IKE-MS	IKE master secret, used for SP800-135 key derivation.
IKE-PSK	IKE Pre-Share Session Key.
KPM-Priv	KPM private key. RSA (n=2048) or ECDSA (P-521) private key used for KMP session establishment
KPM-SENC	AES-256 or 3-Key Triple-DES key for KPM message encryption.
PKI-DMAC	HMAC-SHA1/SHA-256/SHA-384/SHA-512 key used to verify certificate request signature message authenticity.
SNMP-SENC	SNMP (RFC 2574/3414/3826) session encryption key. AES-128 key used to encrypt/decrypt SNMP messages.
SNMP-DMAC	SNMP (RFC 2574/3414/3826) session authentication key. HMAC-SHA-1-96 key used to verify SNMP message authenticity.
MPLS-SENC	MPLS (RFC 3031/3036/3034/3443/2547/4182) session encryption key. AES-128 key used to encrypt/decrypt MPLS messages.
MPLS-DMAC	MPLS (RFC 3031/3036/3034/3443/2547/4182) session encryption key. HMAC-SHA-1 key used to verify MPLS message authenticity.
SSH-DH	SSH Diffie-Hellman private component (2048-bit). Ephemeral DH private key used in SSH.
SSH-Priv	SSH private key. RSA (n=2048) or ECDSA (P-256, P-384) private key used to establish SSH sessions.
SSH-SENC	SSH session encryption key. AES-128, AES-256 or 3-Key Triple-DES key for SSH message encryption/decryption.
SSH-DMAC	SSH session authentication key. HMAC-SHA1/HMAC-SHA-256 session key for SSH message authenticity.
TLS-Host-Priv	AMC TLS private key. RSA (n=2048, n=3072, n=4096) or ECDSA (P-256, P-384) private key used to establish TLS sessions.
TLS-DH-Priv	TLS Diffie-Hellman private component (2048-bit). Ephemeral DH private key used in TLS.
TLS-PMS	TLS pre-master secret (size dependent on the key exchange method) used to derive TLS-SENC and TLS-DMAC.
TLS-SENC	TLS session encryption key. AES-128, AES-256 or 3-Key Triple-DES key for TLS message encryption/decryption.
TLS-DMAC	TLS session authentication key. HMAC-SHA-1/SHA-256 160-bit or 256-bit session key for TLS message authenticity.
AUTH-PW	Authentication Passwords, minimum of 8 characters, printable character set (96 unique values).
External Server Pre-Shared Key	Pre-shared key for RADIUS/TACACS/AD/LDAP server authentication.

Name	Description and Use
TSM Server Pre-Shared Key	TSM server pre-shared key, can use 3-Key Tripe-DES or AES-128 for message encrypt/decrypt, the default is AES-128.
SLOG-SENC	Session log encryption key. AES-256 bit key for session log encryption/decryption.
SLOG-DMAC	HMAC-SHA-256 key used to verify session log message header authenticity.
LDB-DMAC	Log database encryption key. AES-256 bit key for database content encryption/decryption.
SecUpate-Priv	Security update private key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) private key used to digitally sign content security requests.
SecUpdate-SENC	URL filtering or IPS/AV update session encryption Key. AES-128 bit for session message encryption/decryption.
SecUpdate-DMAC	URL filtering or IPS/AV update session authentication key. HMAC-SHA-256 key used to verify session message authenticity.
SSL Proxy Key	SSL proxy encryption/decryption key. The FIPS approved encryption algorithms (AES, Triple-DES) support SSL proxy session encrypt/decrypt.
NTP-ShareKey	HMAC-SHA-256 key used for NTP Message integrity check
RIP-sharekey	HMAC-SHA-256 key used for RIP Message integrity check
OSPF-key	OSPF share key, used for OSPF message integrity check. HMAC-SHA-256 algorithm is used.
keychain	HMAC-SHA-256 used for router protocol Message integrity.

Table 3-9 Public Keys

Name	Description and Use
ROOT-CA	Huawei Root CA. RSA 2048 X.509 Certificate; Used to prove the identity of the device.
PACKAGE-CA	Package CA certificate. RSA 2048 X.509 Certificate; Used to verify the validity of legacy Huawei Images at firmware load.
IKE-Pub	IKE Diffie-Hellman public component. Ephemeral DH public key used in IKE. DH (L= 2048 bit)
SSH-Pub	SSH public key. RSA (n=2048) or ECDSA (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)
TLS-Host-Pub	TLS public key. RSA (n=2048, n=3072, or n=4096) or ECDSA

Name	Description and Use
	(P-521) public key used for TLS session establishment.
TLS-DH-Pub	TLS Diffie-Hellman public component (2048 bit). Ephemeral DH public key used in TLS.
AAPT-CA	Sandbox's CA certificate. When the module and sandbox use HTTPS for data transmission, the module verifies the opposite CA certificate to determine the authenticity of the sandbox.
KPM-Pub	KPM module public key. RSA (n=2048) or ECDSA (P-521) public key used for KPM session establishment.
SecUpdate-Pub	SecUpdate module public key. RSA (n=2048) or ECDSA (P-521) public key used for content security session establishment.

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 VPN End Users and administrative users. 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 (e.g., by organization of the web GUI pages). Authentication status does not persist across module power cycles. To change roles, an operator must first log out, and then log in using another role.

Table 4-1 lists the available roles; the options for authentication types and data are common across roles.

Table 4-1 Roles description

Role		**Authentication**	
ID	**Description**	**Type**	**Data**
Root Administrator (CO)	The Root Administrator role is initially assigned to the default "admin" operator account. It 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*) or Role-based (using *Transitive trust with authentication server*) dependent on the configured policy.	Username and PIN or X.509 certificate
Audit User (AU)	Accesses audit policies and audit logs for diagnostic information.		
API Administrator (AA)	Invokes an API to access the module. Performs only basic network configurations, monitoring and diagnosis, and API administrator configurations. Not available in Approved mode since the API service is disabled by		

Role		Authentication	
	default.		
Administrator (AD)	Configures and monitors the module per delegated access right assigned by the Root Administrator. The role performs most of the system operations except advanced operations, such as creating administrators.		
End User (EU)	FIPS User accessing the virtual private network resources via an encrypted connection.		

4.2 Authentication Methods

Internet access certification mode is configurable, based on the configuration of the authentication strategy. The module provides three authentication mechanisms, including:

- Username and password authentication
- Certificate-base authentication
- Pre-shared key authentication

Table 4-2 lists the relationship of authentication mechanisms with the services and strength of each authentication mechanism.

Table 4-2 Authentication mechanisms for services and strength of mechanisms

Authentication Mechanism	Services	Strength of Mechanism
Username and password authentication	• All available services to CO, AD, and AU, referring to Table 4-3 • Network traffic security (EU) • VPN network traffic-remote VPN access (EU) • VPN network traffic-site to site VPN access (EU)	The minimum password length is eight (8) characters. The password may contain at least three types of the following characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and special characters, allowing for 94 possible characters, with some minor restriction rules. The probability of false authentication is 1/(94^8) ,which is significantly less than 1/1,000,000. The module supports lockout mechanism, which disables a user account after a configured number of unsuccessful attempts to authenticate. A locked-out user cannot successfully log in again until the user account is unlocked. By default, a user is allowed to fail three (3) times per

Authentication Mechanism	Services	Strength of Mechanism
		minute, but this can be configured to allow up to five (5) failed attempts. The probability of false authentication to the module within one minute is 5/(94^8), which is less than 1/100,000. The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data.
Certificate-base authentication	• VPN network traffic-remote VPN access (EU) • VPN network traffic-site to site VPN access (EU)	The module supports certificate-based authentication using 2048 bit RSA keys in FIPS mode. Such keys possess an equivalent strength of 112 bits. The probability of false authentication is 1/(2^112), which is less than 1/1,000,000. The module supports at most 30,000 new sessions per second to authenticate in a one-minute period; so the probability of false authentication to the module within a one-minute period is (60x30,000)/(2^112), which is less than 1/100,000.
Pre-shared key authentication	• VPN network traffic-remote VPN access (EU) • VPN network traffic-site to site VPN access (EU)	The minimum per-shared key length is eight (8) characters. The password may contain at least three (3) types of the following characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and special characters, allowing for 94 possible characters. The odds of guessing a password are 1/(94^8), which is significantly less than 1/1,000,000. The module supports at most 30,000 new sessions per second to authenticate in a one-minute period; so the probability of successfully authenticating to the module within a one-minute period is (60x30,000)/(94^8), which is less than 1/100,000.

4.3 Services

All services implemented by the module are summarized next, with additional detail following #EN-US_TOPIC_0040269395/fig3793169591839 provided for traceability of cryptographic functionality and access to CSPs and public keys by services.

Table 4-3 Authenticated module services

Service	Description	CO	AD	AU	AA	EU
Reset to Factory Defaults	Restoring the module to factory conditions via the CLI command or Web GUI and is the means of providing zeroization keys and CSPs.	X	X[4]			
Module Reset	Rebooting the module via the reset CLI command or WebGUI. This service executes the suite of self-tests required by FIPS 140-2.	X	X			
Configure System (includes Firmware Update)	Update module firmware, license management, SNMP configuration, file management, and logging configuration.	X	X		X	
Configure Network	Network interface configuration and management.	X	X		X	
Configure Policy	VPN access policy configuration.	X	X		X	
Status Monitoring and Reporting	Including Monitor and Dashboard GUI, providing module status (CPU usage, etc.) and logs.	X	X			
Configure audit policy and view audit logs	Including monitoring users' online behavior (HTTP, FTP, QQ and email operations etc.).			X		
Management through API	Including basic network configurations, monitoring and diagnosis, and API administrator configurations.				X	
User Management and Authentication	Creating users, configuring external authentication servers and setting access rights.	X	X[5]		X	
VPN network traffic	Providing VPN services through IPsec, SSL, L2TP, GRE and MPLS.					X
Network traffic security	Traditional firewall features such as application and content filtering, anti-virus, email filtering, IPS, etc.					X

Table 4-4 Unauthenticated module services

Service	Description
Module Reset (Includes Self-test)	Rebooting the module via the reset button. This service executes the suite of self-tests required by FIPS 140-2.
Network Traffic Management	Load balancing, quality of service, bandwidth management and normal traffic.
Show Status	Providing the current status of the cryptographic module.

[[4]] Access level configured by the CO

[[5]] Cannot create additional COsZ

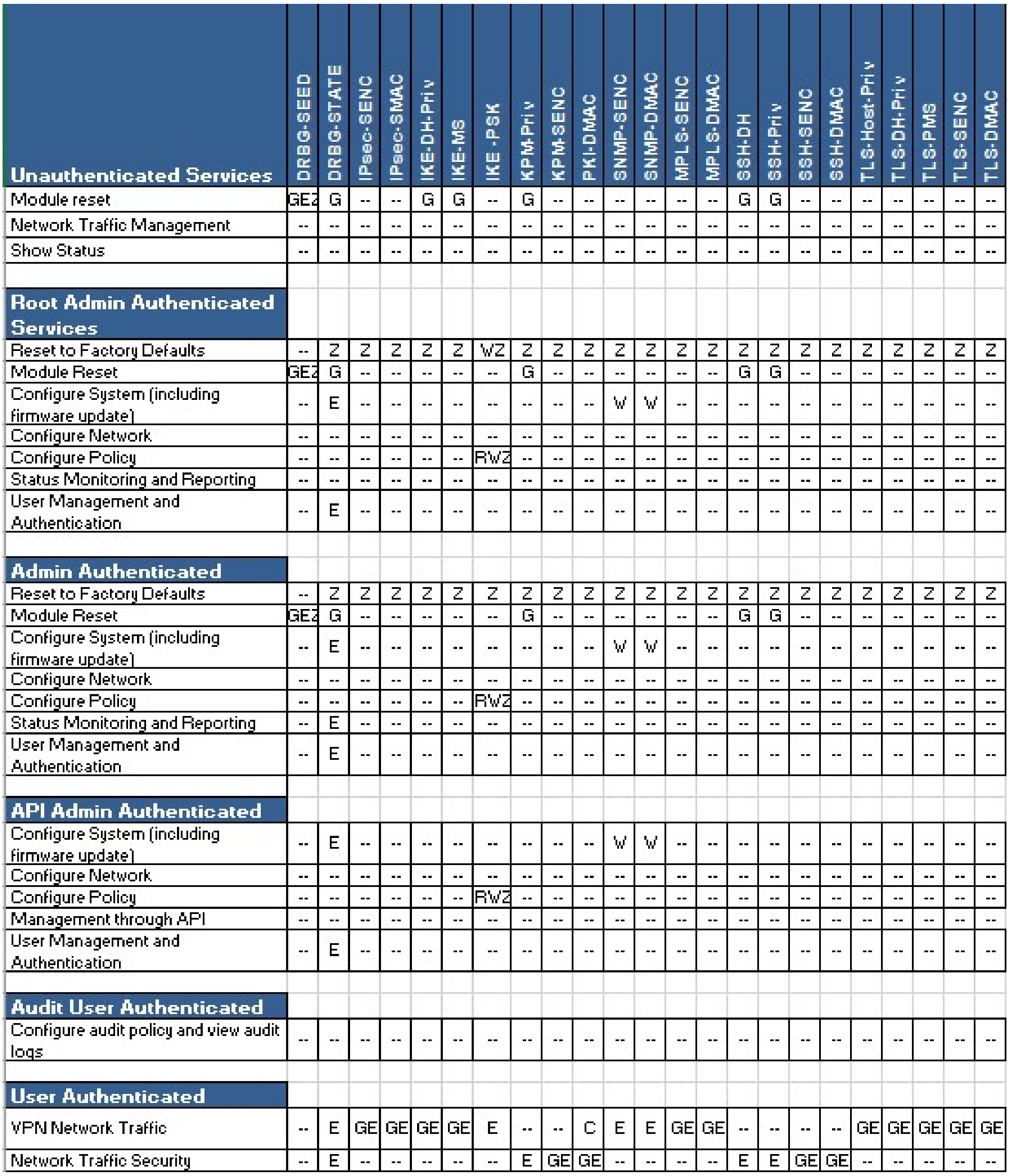
Table 4-5 Services only available in Non-FIPS mode

Services	Description
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, which is a potential security risk.
NETCONF	Invokes an API to access the module
RESTCONF	Invokes an API to access the module
SNMP(v1,v2c)	Configuration, administration and monitoring
FTP	Using ftp to transfer file in plain text is a potential security risk
SSHv1.0 SSHv1.5	It's not safe to connect to remote machine via SSHv1
PKI (Key Pair Create)	Running the command "pki rsa local-key-pair create *key-name*" is not allowed in FIPS mode.

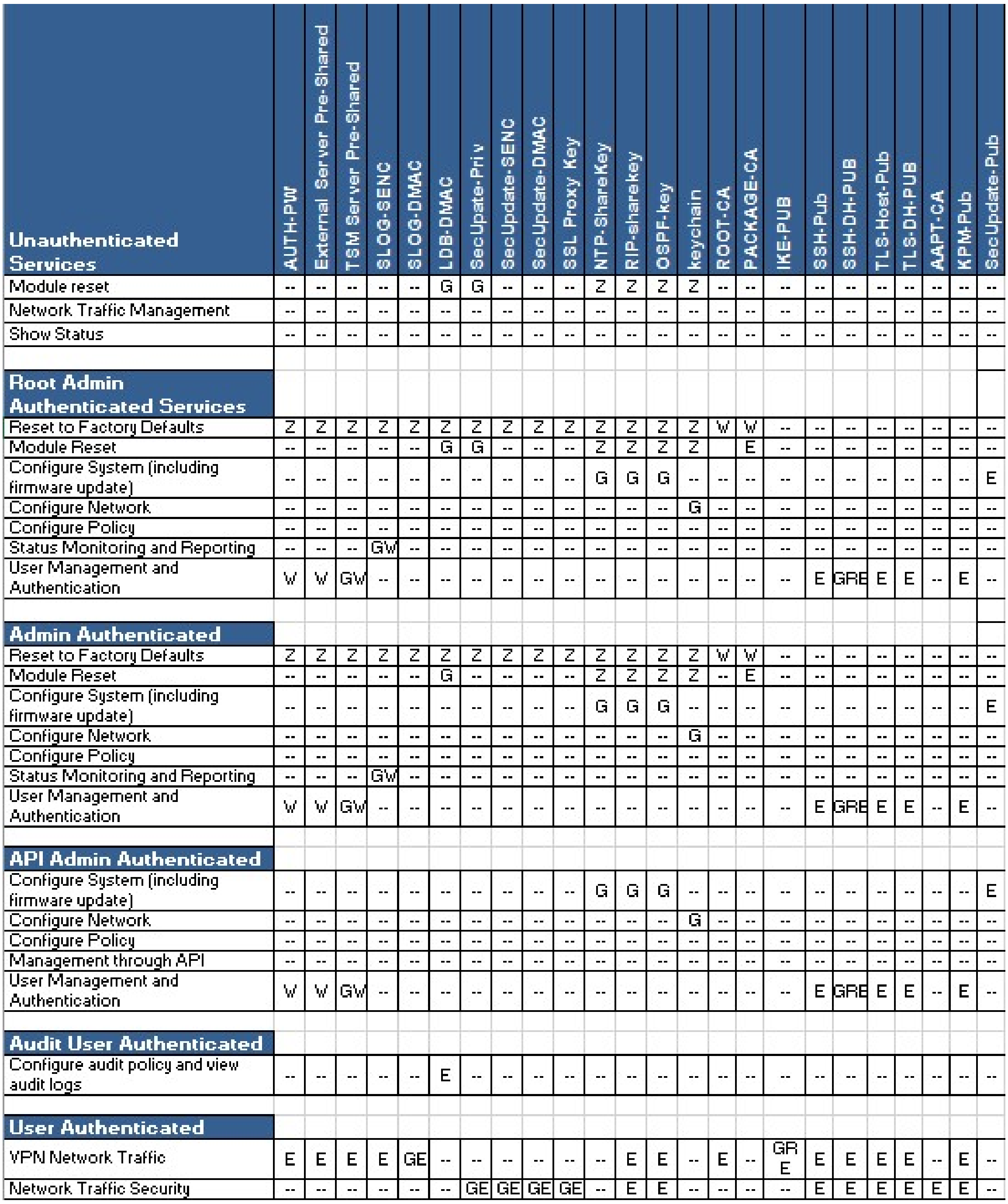
Figure 4-1 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP (unmodified output of DRBG).
- 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.

Figure 4-1 CSP access rights within services



Unauthenticated Services	DRBG-SEED	DRBG-STATE	IPsec-SENC	IPsec-SMAC	IKE-DH-Priv	IKE-MS	IKE-PSK	KPM-Priv	KPM-SENC	PKI-DMAC	SNMP-SENC	SNMP-DMAC	MPLS-SENC	MPLS-DMAC	SSH-DH	SSH-Priv	SSH-SENC	SSH-DMAC	TLS-Host-Priv	TLS-DH-Priv	TLS-PMS	TLS-SENC	TLS-DMAC
Module reset	GEZ	G	--	--	G	G	--	G	--	--	--	--	--	--	G	G	--	--	--	--	--	--	--
Network Traffic Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Root Admin Authenticated Services																							
Reset to Factory Defaults	--	Z	Z	Z	Z	Z	WZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Module Reset	GEZ	G	--	--	--	--	--	G	--	--	--	--	--	--	G	G	--	--	--	--	--	--	--
Configure System (including firmware update)	--	E	--	--	--	--	--	--	--	--	W	W	--	--	--	--	--	--	--	--	--	--	--
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure Policy	--	--	--	--	--	--	RWZ	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status Monitoring and Reporting	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Admin Authenticated																							
Reset to Factory Defaults	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Module Reset	GEZ	G	--	--	--	--	--	G	--	--	--	--	--	--	G	G	--	--	--	--	--	--	--
Configure System (including firmware update)	--	E	--	--	--	--	--	--	--	--	W	W	--	--	--	--	--	--	--	--	--	--	--
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure Policy	--	--	--	--	--	--	RWZ	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status Monitoring and Reporting	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
API Admin Authenticated																							
Configure System (including firmware update)	--	E	--	--	--	--	--	--	--	--	W	W	--	--	--	--	--	--	--	--	--	--	--
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure Policy	--	--	--	--	--	--	RWZ	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Management through API	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Audit User Authenticated																							
Configure audit policy and view audit logs	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Authenticated																							
VPN Network Traffic	--	E	GE	GE	GE	GE	E	--	--	C	E	E	GE	GE	--	--	--	--	GE	GE	GE	GE	GE
Network Traffic Security	--	E	--	--	--	--	--	E	GE	GE	--	--	--	--	E	E	GE	GE	--	--	--	--	--



Unauthenticated Services	AUTH-PW	External Server Pre-Shared	TSM Server Pre-Shared	SLOG-SENC	SLOG-DMAC	LDB-DMAC	SecUpate-Priv	SecUpdate-SENC	SecUpdate-DMAC	SSL Proxy Key	NTP-ShareKey	RIP-sharekey	OSPF-key	keychain	ROOT-CA	PACKAGE-CA	IKE-PUB	SSH-Pub	SSH-DH-PUB	TLS-Host-Pub	TLS-DH-PUB	AAPT-CA	KPM-Pub	SecUpdate-Pub
Module reset	--	--	--	--	--	G	G	--	--	--	Z	Z	Z	Z	--	--	--	--	--	--	--	--	--	--
Network Traffic Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Root Admin Authenticated Services																								
Reset to Factory Defaults	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	W	W	--	--	--	--	--	--	--	--
Module Reset	--	--	--	--	--	G	G	--	--	--	Z	Z	Z	Z		E	--	--	--	--	--	--	--	--
Configure System (including firmware update)	--	--	--	--	--	--	--	--	--	--	G	G	G	--	--	--	--	--	--	--	--	--	--	E
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	G	--	--	--	--	--	--	--	--	--	--
Configure Policy	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status Monitoring and Reporting	--	--	--	GW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	W	W	GW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	GRE	E	E	--	E	--
Admin Authenticated																								
Reset to Factory Defaults	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	W	W	--	--	--	--	--	--	--	--
Module Reset	--	--	--	--	--	G	--	--	--	--	Z	Z	Z	Z	--	E	--	--	--	--	--	--	--	--
Configure System (including firmware update)	--	--	--	--	--	--	--	--	--	--	G	G	G	--	--	--	--	--	--	--	--	--	--	E
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	G	--	--	--	--	--	--	--	--	--	--
Configure Policy	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status Monitoring and Reporting	--	--	--	GW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	W	W	GW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	GRE	E	E	--	E	--
API Admin Authenticated																								
Configure System (including firmware update)	--	--	--	--	--	--	--	--	--	--	G	G	G	--	--	--	--	--	--	--	--	--	--	E
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	G	--	--	--	--	--	--	--	--	--	--
Configure Policy	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Management through API	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	W	W	GW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	GRE	E	E	--	E	--
Audit User Authenticated																								
Configure audit policy and view audit logs	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Authenticated																								
VPN Network Traffic	E	E	E	E	GE	--	--	--	--	--	--	E	E	--	E	--	GRE	E	E	E	E	--	E	--
Network Traffic Security	--	--	--	--	--	--	GE	GE	GE	GE	--	E	E	--	--	--	--	E	E	E	E	E	E	--

The Module Reset service instantiates the DRBG, with 262,144 bit entropy input (DRBG-EI) produced by the Allowed NDRNG. The generation of DRBG-State uses the [SP 800-90A] CTR_DRBG (AES256). The Zeroization of session keys by this service covers the case of module shutdown or power-cycle while a secure channels session (SSH, TLS, IPsec or SNMP) is active.

The *Show Status* service and *Network Traffic Management* service do not access CSPs or public keys.

There is a limit of 2^28 encryptions with the same Triple-DES key. The user is responsible for ensuring the module does not surpass this limit.

5 Self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data has 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 below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the self-test is interrupted, and the module enters the Critical Failure error state.

Table 5-1 Power-up self-tests

Test Target (Cert. #)	Description
BOOTROM	Integrity check with 16-bit CRC.
Firmware Integrity	Integrity check with digital signature (cms) using RSA (2048) and SHA256.
AES OpenSSL (#4449)	Separate encrypt, decrypt KATs using 256-bit keys CBC.
AES VPP (#4451)	Separate encrypt, decrypt KATs using 256-bit keys CBC and 256-bit keys CFB.
DRBG OpenSSL (#1440)	AES-256 CTR DRBG test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90 Section 11.3.
DRBG VPP (#1442)	AES-256 CTR DRBG test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90 Section 11.3.
HMAC OpenSSL (#2952)	Separate HMAC generation and verification KATs, using SHA-256
HMAC VPP (#2954)	Separate HMAC generation and verification KATs, using SHA-256
RSA OpenSSL (#2430)	Separate KATs of n=2048 bit signature generation and signature verification.
RSA VPP (#2432)	Separate KATs of n=2048 and n=3072 bit signature generation and signature verification.

Test Target (Cert. #)	Description
SHS OpenSSL (#3662)	Separate KATs of SHA-1, SHA-256, SHA-512
SHS VPP (#3664)	Separate KATs of SHA-1, SHA-256, SHA-512
Triple-DES OpenSSL (#2391)	Separate encrypt, decrypt KATs using 3-key TCBC.
Triple-DES VPP (#2393)	Separate encrypt, decrypt KATs using 3-key TCBC.
ECDSA VPP(#1084)	Signature generation and signature verifications using P-256 and SHA256.
AES GCM OpenSSL (#4449 and #4450)	Separate encrypt and decrypt, 256 key length.
ECDH OpenSSL (#1149)	Shared secret calculation using P-256 KAT.
ECDH VPP (#1153)	Shared secret calculation using P-256 KAT.

Table 5-2 Conditional self-tests

Test Target	Description
NDRNG	AS09.42 Continuous RNG Test performed on each NDRNG access.
DRBG	AS09.42 Continuous RNG Test performed on each DRBG access.
RSA	RSA Pairwise Consistency Test performed on each RSA key pair generation.
ECDSA	Pairwise consistency test on each generation of a key pair.
Patch, Module and Firmware	Integrity check with digital signature (cms) using RSA (2048) and SHA256.

If all power-up self-tests succeed, the system will display the following message on the console.

```
FIPS power-up self-test end...passed
```

If any of the power-up self-tests fails, the module enters an error state. The following error message would be seen on the console and the module would be forced to reboot.

```
Self-tests failed!
The system will reboot.(Reason=Self-tests failed)
```

If any of the conditional tests fails, the system will display the following error message of the specific condition.

```
condutional-test-name conditional tests failed!
```

6 Physical Security Policy

6.1 Physical Security Mechanisms

The cryptographic modules each include the following physical security mechanisms:

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

The USG6310S/6370/6620/6650/6680 is a multi-chip standalone module that production quality contains standard passivation. Chip components are protected by external baffles. There are tamper seals that are applied on the modules by the CO. All unused seals are to be controlled by the CO. The seals prevent removal of the opaque enclosure without evidence. The CO must ensure that the module surface is clean and dry. Tamper evident labels must be pressed firmly onto the adhering surfaces during installation and once applied the CO shall permit 24 hours of cure time for all tamper evident labels. The CO should inspect the seals and shields for evidence of tamper every 30 days. If the seals show evidence of tamper, the CO should assume that the modules have been compromised and contact Customer Support.

NOTE

For ordering information of external baffles and tamper seals, see Table 2-2.

6.2 External Baffle Placement

In order to mitigate the risk of determining the composition or implementation of the module due to heat dissipation holes, external baffles or opaque enclosures shall be installed in the following locations:

- On both sides of the USG6310S/6370/6620/6650/6680 chassis

To prevent the determination of the composition or implementation of the module, the USG6310S/6370/6620/6650/6680 models need to be installed with external baffles.

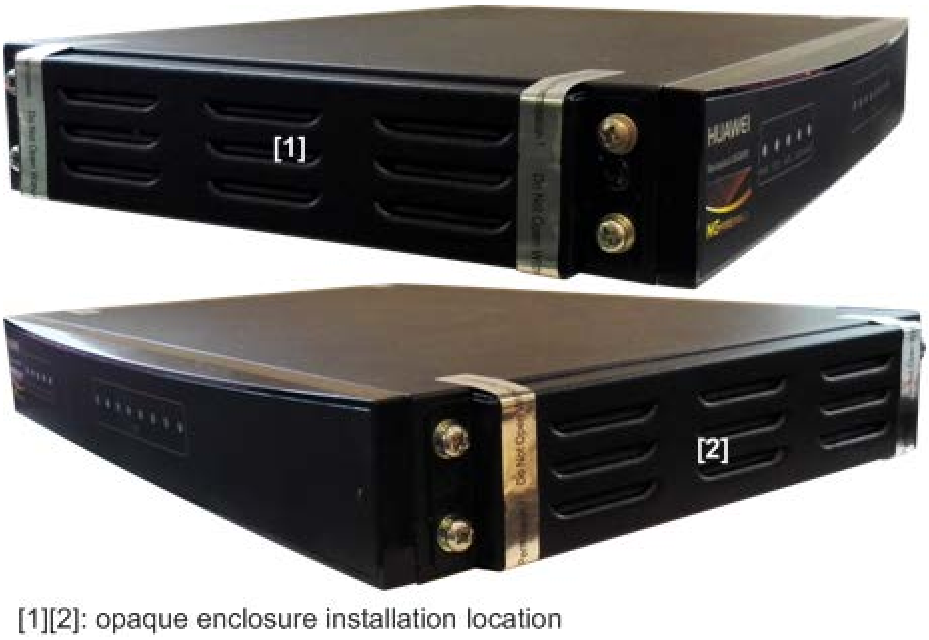
NOTE

After the external baffles have been applied to the USG6310S/6370/6620/6650/6680 models, the operational temperature range will be 0°C to 40°C.

The following is the installation locations for each model’s opaque enclosure (external baffle).

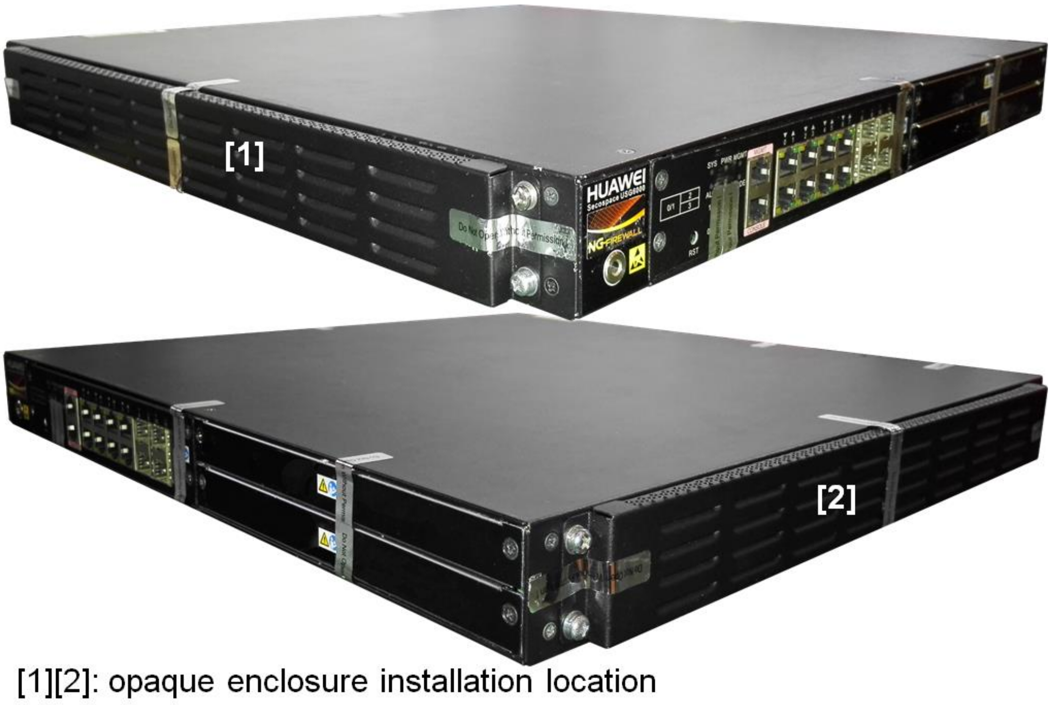
USG6310S

Figure 6-1 USG6310S external baffle placement



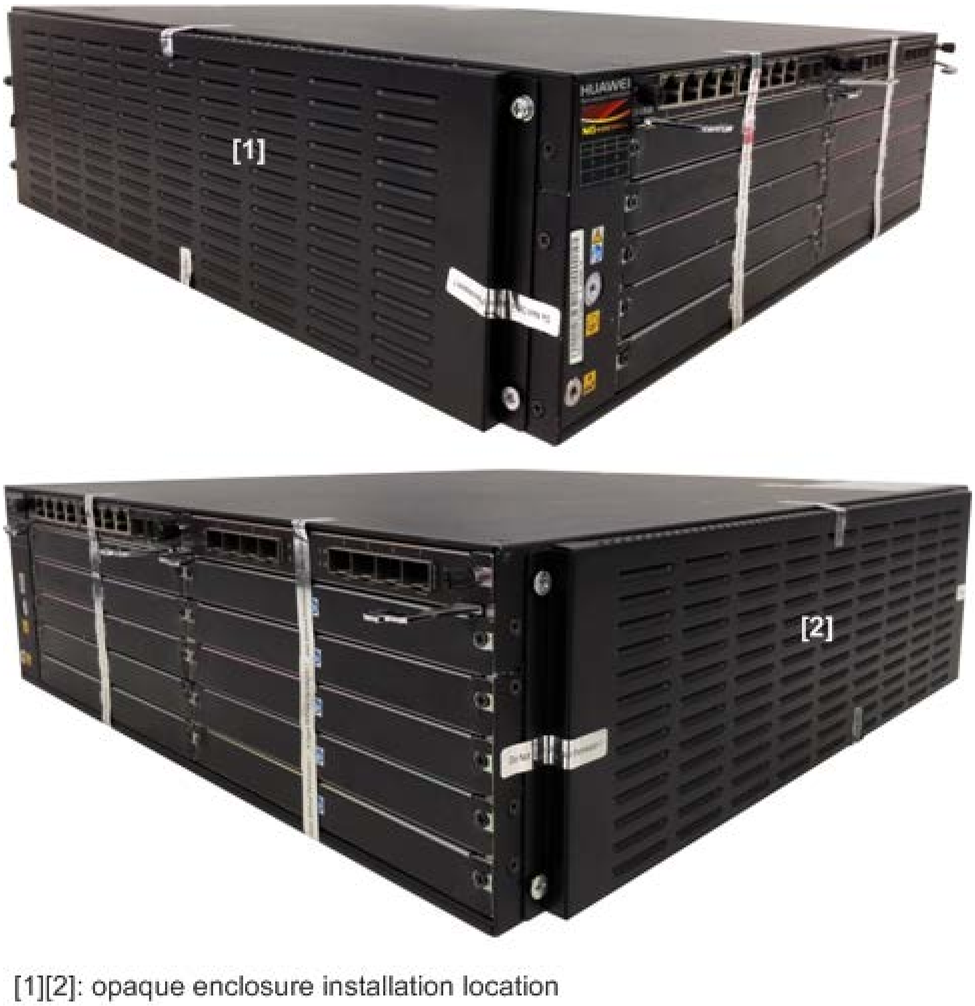
USG6370 and USG6620

Figure 6-2 USG6370/6620 external baffle placement



USG6650

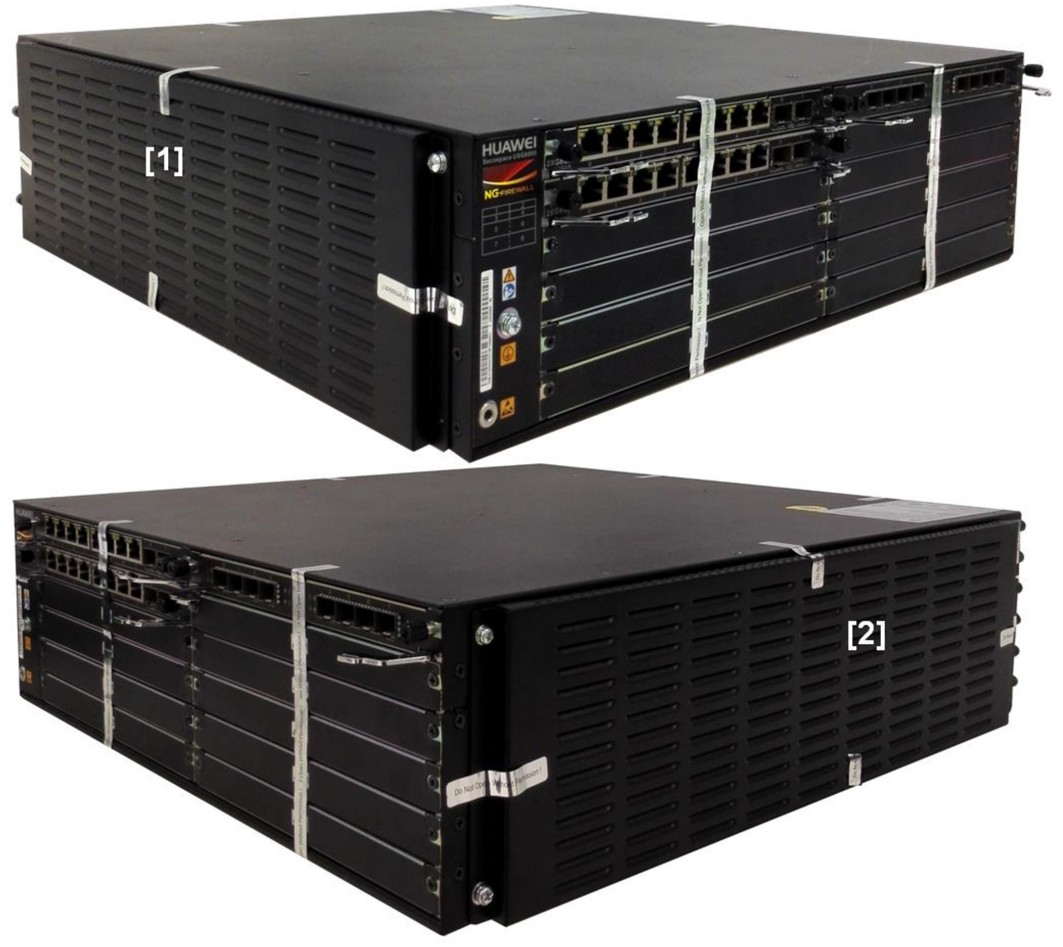
Figure 6-3 USG6650 external baffle placement



[1][2]: opaque enclosure installation location

USG6680

Figure 6-4 USG6680 external baffle placement



[1][2]: opaque enclosure installation location

6.3 Tamper Seal Placement

The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. This section includes the installation locations for each model’s tamper seals.

USG6310S

The USG6310S includes thirteen (13) tamper-evident seals, which are applied to the USG6310S as follows:

- Two (2) seals applied to top lid and right side baffle (see #1 and #3 in Figure 6-5
- Two (2) seals applied to bottom and right side baffle (see #2 and #4 in Figure 6-5 and Figure 6-7)
- Two (2) seals applied to top lid and left side baffle (see #5 and #7 in Figure 6-5)
- Two (2) seals applied to bottom and left side baffle (see #6 and #8 in Figure 6-5 and Figure 6-7)
- Four (4) seals applied to back and bottom, preventing port access (see #9 to #12 in Figure 6-6)
- One (1) seal applied to the bottom and the bottom of the front faceplate (see #13 in Figure 6-7)

Figure 6-5 USG6310S tamper seal placement- right and left sides

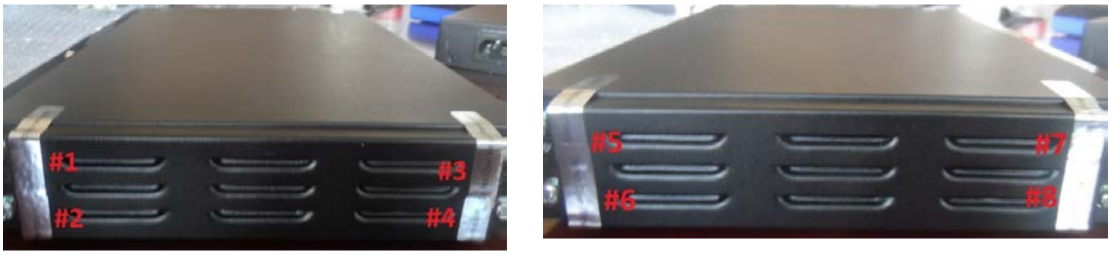


Figure 6-6 USG6310S tamper seal placement- back

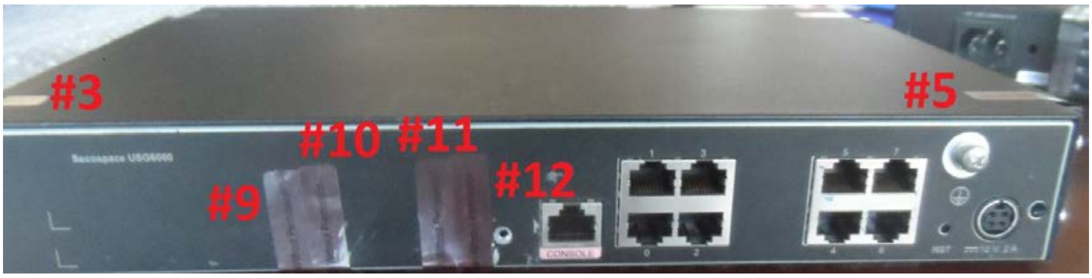
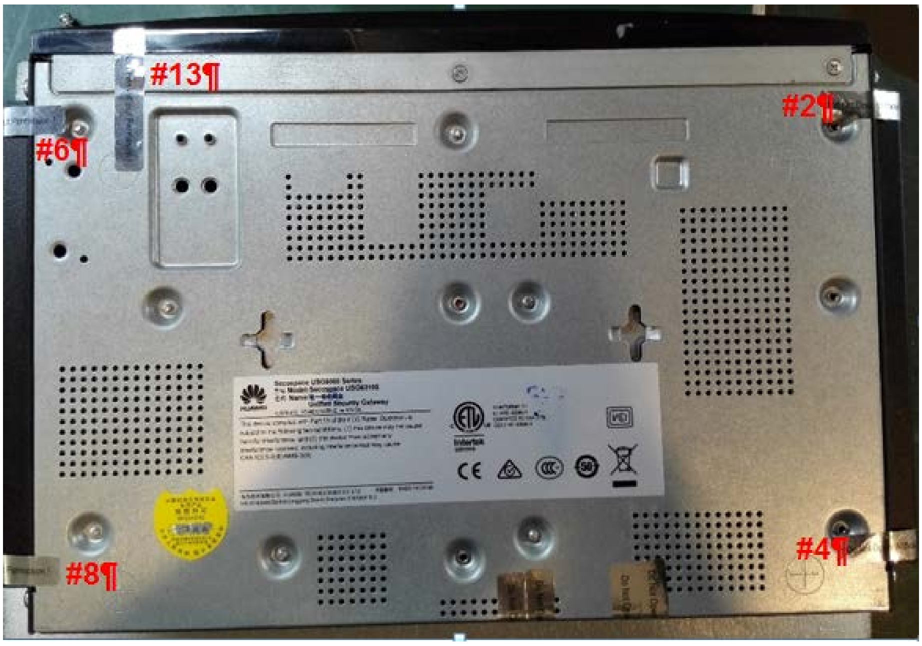


Figure 6-7 USG6310S tamper seal placement- bottom



USG6370 and USG6620

The USG6370 and USG6620 models each include nineteen (19) tamper-evident seals, which are applied to each model as follows:

- Two (2) seals applied to the front plate and bottom, preventing port access (see [#1] & [#2] in Figure 6-8 and Figure 6-8)
- One (1) seal applied to the front and top lid, covering a screw (see #3 in Figure 6-8 and Figure 6-12)
- One (1) seal applied to the front and bottom, covering a screw (see #4 in Figure 6-8 and Figure 6-13)
- One (1) seal applied to the front and bottom (see #5 in Figure 6-8 and Figure 6-13)
- One (1) seal applied to the front and top lid (see #6 in Figure 6-8 and Figure 6-12)
- One (1) seal applied to the back and top lid (#7 in Figure 6-9 and Figure 6-12)
- One (1) seal applied to the back and bottom (#8 in Figure 6-9 and Figure 6-13)
- One (1) seal applied to the back and top lid (#9 in Figure 6-9 and Figure 6-12)
- One (1) seal applied to the back and bottom (#10 in Figure 6-9 and Figure 6-13)
- One (1) seal applied to the back and bottom, covering the power supply (#11 in Figure 6-9 and Figure 6-13)
- Two (2) seals applied to the right side baffle and the main module (see #12 and #15 in Figure 6-10)
- Two (2) seals applied to the left side baffle and the main module (see #16 and #19 in Figure 6-11)
- One (1) seal applied to the top lid and right baffle (see #13 in Figure 6-10 and Figure 6-12)

- One (1) seal applied to the bottom and right baffle (see #14 in Figure 6-10 and Figure 6-13)
- One (1) seal applied to the top and left baffle (see #17 in Figure 6-11 and Figure 6-12)
- One (1) seal applied to the bottom and left baffle (see #18 in Figure 6-11 and Figure 6-13)

Note:

- For the locations numbered [#12]-[#19], install the external baffles and then apply the tamper seals. Other locations are directly covered with the tamper seals.
- WSIC slots are reserved for expansion cards to provide more ports or functions. By default, the filler panel is installed on the WSIC slot. When a WSIC card is purchased, tamper seals need to be applied after installing the card (refer to [#5] & [#6] in Figure 6-8).
- The USG6370 and USG6620 both support optional hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B. Hard disks are used to store logs and reports, and they can be purchased from Huawei if necessary. When a hard disk combination is purchased, tamper seals need to be applied after installing the hard disk (refer to [#7] & [#9] in Figure 6-8.

Figure 6-8 USG6370/6620 tamper seal placement- front

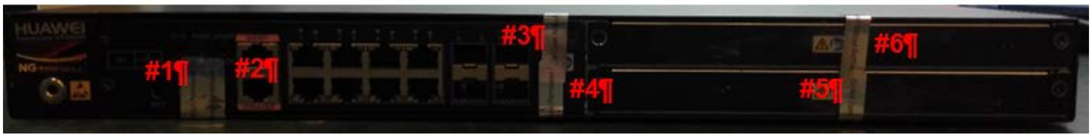


Figure 6-9 USG6370/6620 tamper seal placement- back

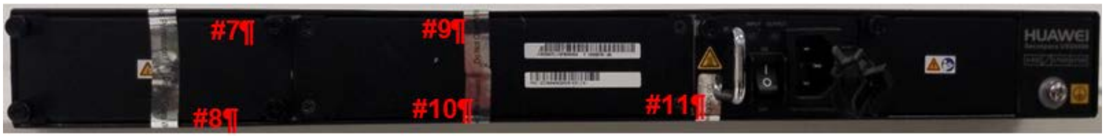


Figure 6-10 USG6370/6620 tamper seal placement- right side

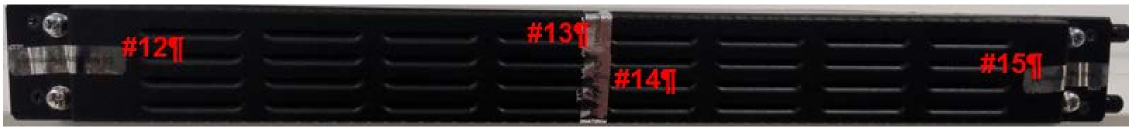


Figure 6-11 USG6370/6620 tamper seal placement- left side

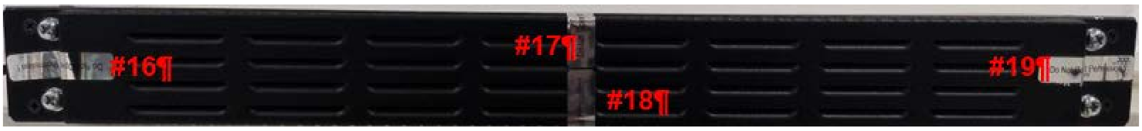


Figure 6-12 USG6370/6620 tamper seal placement- top

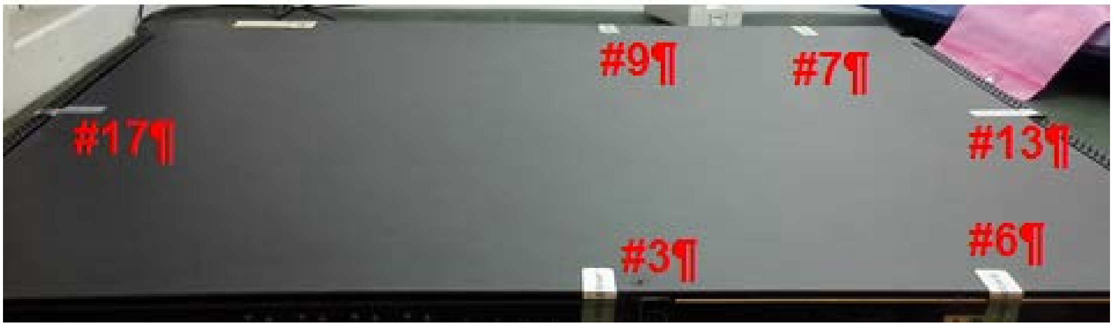
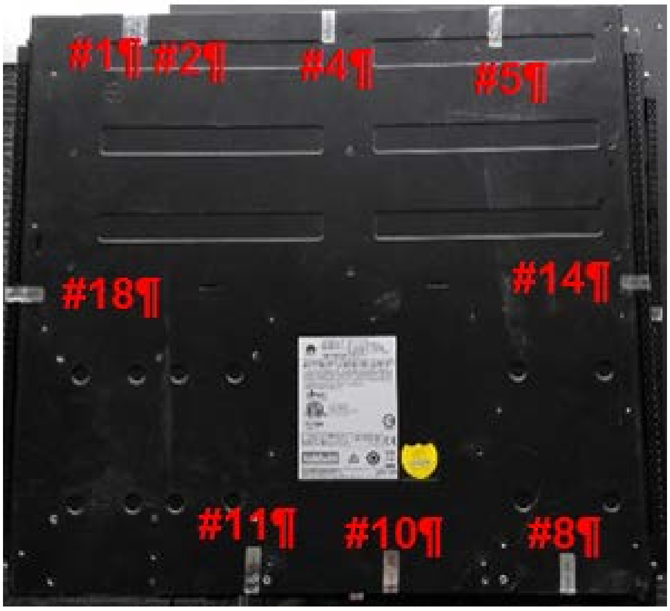


Figure 6-13 USG6370/6620 tamper seal placement- bottom



USG6650 and USG6680

The USG6650 and USG6680 models each include twenty-five (25) tamper-evident seals, which are applied to the each model as follows:

- Two (2) seals applied to front cards and top lid (see #1 and #5 in Figure 6-14 and Figure 6-18)
- Four (4) seals applied to front faceplates (see #2, #3, #6, and #7 in Figure 6-14)
- Two (2) seals applied to front faceplates and bottom (see #4 and #8 in Figure 6-14 and Figure 6-19)
- Two (2) seals applied to back faceplates and top lid (see #9 and #10 in Figure 6-15 and Figure 6-18)
- Six (6) seals applied to back faceplates (see #11 to #16 in Figure 6-15)
- One (1) seal applied to back faceplate and bottom (see #17 in Figure 6-15 and Figure 6-19)
- Two (2) seals applied to right baffle and main module (see #18 and #21 in Figure 6-16)

- One (1) seal applied to right baffle and top lid (see #19 Figure 6-16 and Figure 6-18)
- One (1) seal applied to right baffle and bottom (see #20 in Figure 6-16 and Figure 6-19)
- Two (2) seals applied to left baffle and main module (see #22 and #25 in Figure 6-17)
- One (1) seal applied to left baffle and top lid (see #23 Figure 6-17 and Figure 6-18)
- One (1) seal applied to left baffle and bottom (see #24 in Figure 6-17 and Figure 6-19)

Note:

- For the locations numbered [#18]-[#25], install the opaque enclosures, and then apply the tamper seals.
- WSIC slots are reserved for expansion cards to provide more ports or functions. By default, the filler panel is installed on the WSIC slot. When a WSIC card is purchased, tamper seals need to be applied after installing the card (refer to [#2-#4]-[#6-#8] in Figure 6-14).
- The USG6650 and the USG6680 both support SM-HDD-SAS300G-A/SM-HDD-SAS600G-A/SM-HDD-SAS1200G-A hard disks. The hard disks are optional. Hard disks are used to store logs and reports. You can purchase one or two hard disks from Huawei if needed. To ensure hard disk data reliability, you are advised to purchase two hard disks with the same capacity to create RAID1 for data backup. When you purchase hard disks, you need tamper seals after installation of the hard disks (refer to [#11, #12, #14 and #15] in Figure 6-14).

Figure 6-14 USG6650/USG6680 tamper seal placement- front

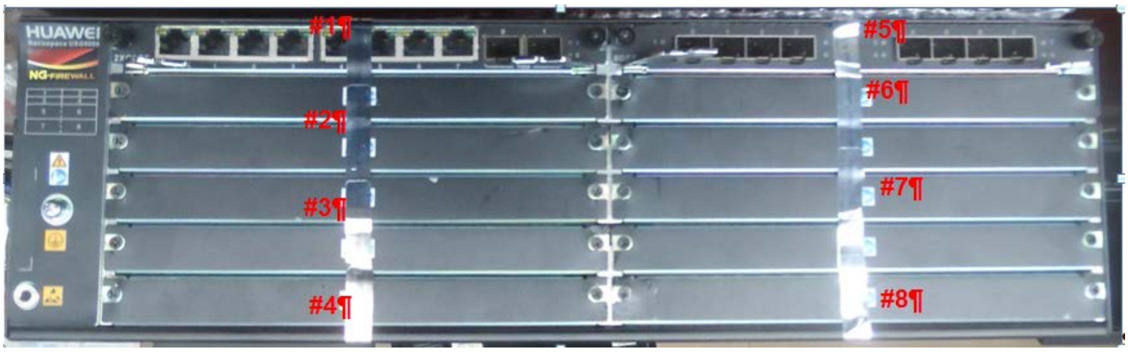


Figure 6-15 USG6650/USG6680 tamper seal placement- back

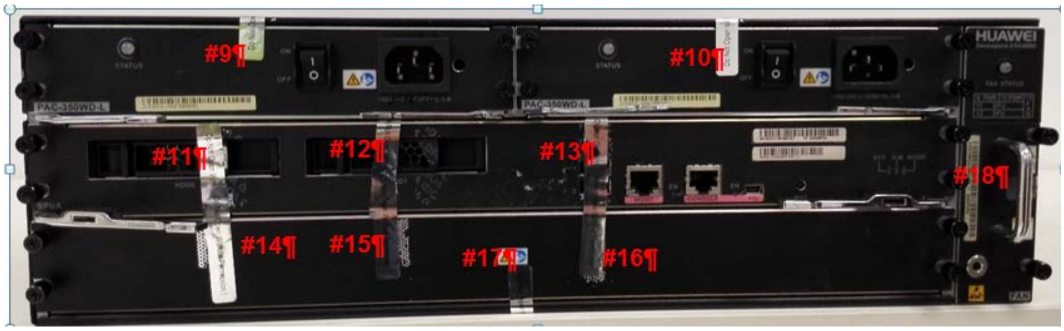


Figure 6-16 USG6650/USG6680 tamper seal placement- right side

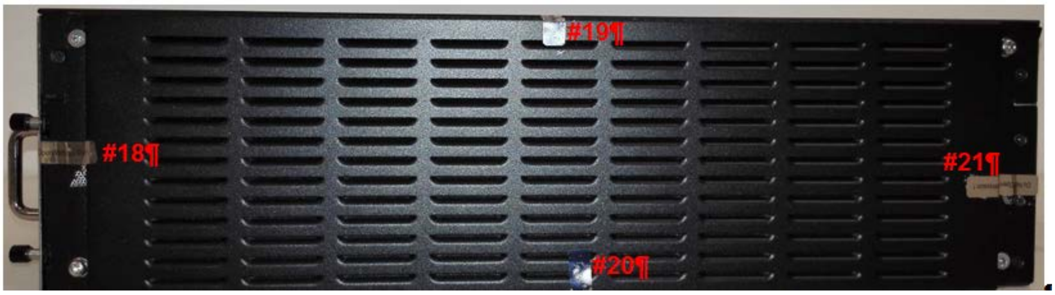


Figure 6-17 USG6650/USG6680 tamper seal placement- left side

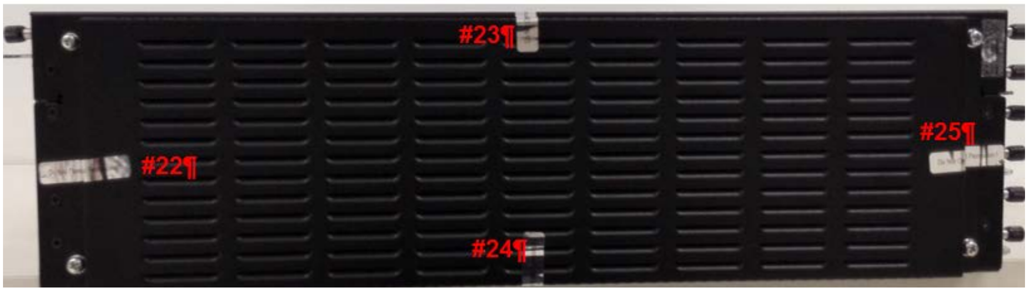


Figure 6-18 USG6650 /USG6680 tamper seal placement- top

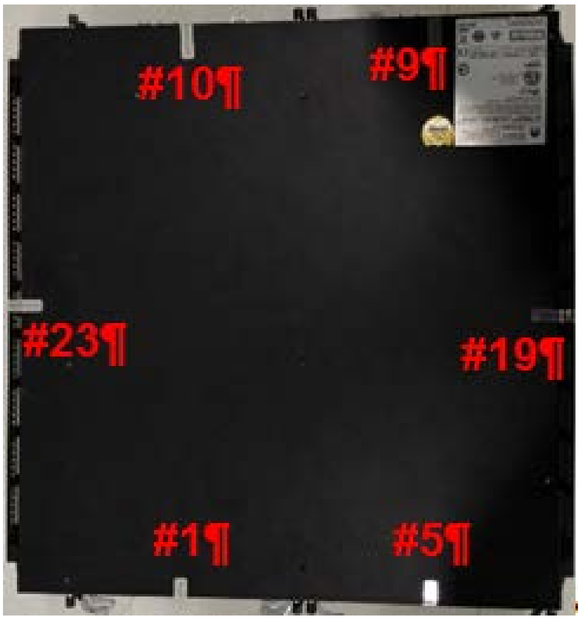
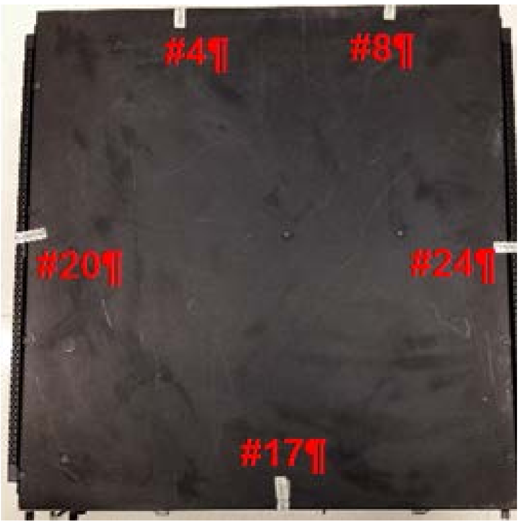


Figure 6-19 USG6650/USG6680 tamper seal placement- bottom



7 Operational Environment

The module is designated as a limited operational environment under the FIPS 140-2 definitions. For details, see the statement in Section 2 Introduction.

8 Mitigation of Other Attacks Policy

The module has 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:

- An unauthenticated operator does not have access to any CSPs or cryptographic services.
- The module inhibits data output during power-up self-tests and error states.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- Zeroization overwrites all CSPs.
- The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation.

To switch the module from Non-FIPS mode to Approved mode, reset the module to factory defaults. And the following security rules must be adhered to for operation in the FIPS 140-2 Approved mode:

1. Configure the module to only use SNMP v3:

```
<sysname> system-view
[sysname] snmp-agent
[sysname] snmp-agent sys-info version v3
[sysname] undo snmp-agent sys-info version v1
[sysname] undo snmp-agent sys-info version v2c
```

2. Configure SNMP v3 to use only approved primitives (AES, SHA).

```
<sysname> system-view
[sysname] snmp-agent group v3 testgroup privacy
[sysname] snmp-agent usm-user v3 testuser group testgruop
```

Warning: Adding the user to a privacy group is recommended, because the bound group has insecure properties (with authentication or no-authentication configured).

```
[sysname] snmp-agent usm-user v3 testuser authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[sysname] snmp-agent usm-user v3 testuser privacy-mode aes2128
Please configure the privacy password (8-64)
```

The snmp-agent's privacy-mode can be set to aes128. So the administrator can change the preference of SNMP user's encryption algorithms using the upper second command.

3. Configure the SSH server to only support SSH v2.

```
<sysname> system-view
[sysname] undo ssh server compatible-ssh1x enable
[sysname] ssh server key-exchange dh_group_exchange_sha1 dh_group14_sha1
[sysname] ssh server hmac sha2_256 sha2_256_96 sha1 sha1_96
[sysname] ssh server cipher aes256_ctr aes128_ctr aes256_cbc aes128_cbc 3des_cbc
```

4. Configure the cipher suite for the customized SSL cipher-suite policy, and bind the SSL cipher-suite policy to an SSL policy to disable the SSL versions lower than v3.1.

```
<sysname> system-view
[sysname] ssl cipher-suite-list cipher1
[sysname-ssl-cipher-suite-cipher1] set cipher-suite
tls12_ck_rsa_aes_256_cbc_sha256
[sysname-ssl-cipher-suite-cipher1] set cipher-suite tls1_ck_rsa_with_aes_128_sha
[sysname-ssl-cipher-suite-cipher1] set cipher-suite tls1_ck_rsa_with_aes_256_sha
[sysname-ssl-cipher-suite-cipher1] set cipher-suite
tls1_ck_dhe_rsa_with_aes_128_sha
[sysname-ssl-cipher-suite-cipher1] set cipher-suite
tls1_ck_dhe_rsa_with_aes_256_sha
[sysname-ssl-cipher-suite-cipher1] quit
[sysname] ssl policy test
[sysname-ssl-policy-test] ssl minimum version tls1.0
[sysname-ssl-policy-test] binding cipher-suite-customization cipher1
```

5. Configure the decrypted traffic detection profile for SSL decryption policy to refer. The application scenario can be **inbound**, **outbound** or **no-decrypt** based on the configurations.

```
<sysname> system-view
[sysname] profile type decryption name prof1
[sysname-profile-decryption-prof1]detect type inbound
[sysname-profile-decryption-prof1] ssl-cipher client-side user-defined AES256-SHA:
AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:AES256-SHA256
[sysname-profile-decryption-prof1] ssl-cipher server-side user-defined AES256-SHA:
AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:AES256-SHA256
[sysname-profile-decryption-prof1] ssl-version client-side tls1.0 tls1.1 tls1.2
ssl3.0
[sysname-profile-decryption-prof1] ssl-version server-side tls1.0 tls1.1 tls1.2
ssl3.0
```

6. Configure an IPsec proposal and define security parameters for IPsec SA negotiation, including the security protocol (ESP), encryption and authentication algorithms. Both ends of an IPsec tunnel must be configured with the same parameters.

```
<sysname> system-view
[sysname] ipsec proposal newprop1
[sysname-ipsec-proposal-newprop1] transform esp
[sysname-ipsec-proposal-newprop1] esp authentication-algorithm sha2-256 sha2-384
sha2-512 sha1
[sysname-ipsec-proposal-newprop1] esp encryption-algorithm aes-128
aes-128-gcm-128 aes-192 aes-192-gcm-128 aes-256 aes-256-gcm-128 3des
```

Cofigure an IKE proposal and define security parameters for IKE peer, including the encryption algorithm, authentication method, authentication algorithm ,DH group and SA lifetime.

```
<sysname> system-view
[sysname] ike proposal ike_prop
[sysname-ike-proposal-ike_prop] encryption-algorithm aes-256 aes-192 aes-128 3des
[sysname-ike-proposal-ike_prop] authentication-algorithm sha2-512 sha2-384
sha2-256 sha1
```

```
[system-ike-proposal-ike_prop] integrity-algorithm hmac-sha2-256 hmac-sha2-384
hmac-sha2-512
[sysname-ike-proposal-ike_prop] prf hmac-sha1 hmac-sha2-256 hmac-sha2-384
hmac-sha2-512
[sysname-ike-proposal-ike_prop] dh group14 group15 group16 group19 group20 group21
```

7. For SSL VPN configuration, the module supports the aes256-sha and aes128-sha algorithms by default. You can run the following commands to prohibit the non-FIPS algorithms.

```
<sysname> system-view
[sysname] v-gateway abc
[sysname-abc] basic
[sysname-abc-basic] ssl ciphersuit custom aes256-sha non-des-cbc3-sha non-rc4-sah
aes256-sha
```

8. Establish the connection between the Radius, HWtacacs, AD, LDAP, and TSM servers and the module with a secure channel (to prevent the output of passwords in plain text).

   – AD:

     The AD server authentication contains the Kerberos authentication and standard LDAP authentication processes. The server verifies the administrator DN and password that the module uses to access the AD server to verity client legitimacy. You can configure LDAP over SSL (LDAPS) to use SSL to enhance security in the LDAP process. The administrator password must contain at least 8 characters in at least three of the following types of characters: lower-case letters, upper-case letters, digits, and special characters.

```
<sysname> system-view
[sysname] ad-server template template1
[sysname-ad-template1] ad-server authentication manager cn=manager password
[ repassword ]
[sysname-ad-template1]ad-server authentication <ip-address> ldap-over-ssl
```

   – LDAP:

     The LDAP server verifies the administrator DN and password configured on the module to verity client legitimacy. You can also configure LDAP over SSL (LDAPS) to use SSL to enhance security. The administrator password must contain at least 8 characters in at least three of the following types of characters: lower-case letters, upper-case letters, digits, and special characters.

```
<sysname> system-view
[sysname] ldap-server template template1
[sysname-ldap-template1] ldap-server authentication manager cn=manager
password [ repassword ]
[sysname-ldap-template1]ldap-server authentication <ip-address> ssl
```

   – TSM:

     The module and TSM server use a shared key to exchange authentication messages. To ensure validity of both communication parties, the module and TSM server must be configured with the same shared key. The key must contain at least 8 characters in at least three of the following types of characters: lower-case letters, upper-case letters, digits, and special characters.

```
<sysname> system-view
[sysname] tsm-server template test
[sysname-tsm-test] tsm-server encryption-mode aes128 shared-key shared-key
```

     It's ok to change the preference of encryption-mode to 3DES by command "**tsm-server encryption-mode 3des**".

For Radius and HWtacacs server authentication, the servers interact with our module over IPSec.

- Radius

  The module and RADIUS server use a shared key to exchange authentication messages. To ensure validity of both communication parties, the module and RADIUS server must be configured with the same shared key. The key must contain at least 8 characters in at least three of the following types of characters: lower-case letters, upper-case letters, digits, and special characters.

  ```
  <sysname>  system-view
  [sysname] radius-server template template1
  [sysname-radius-template] radius-server shared-key cipher key-string
  ```

- HWTACACS:

  The module and HWTACACS server use a shared key to exchange authentication messages. To ensure validity of both communication parties, the module and HWTACACS server must be configured with the same shared key. The key must contain at least 8 characters in at least three of the following types of characters: lower-case letters, upper-case letters, digits, and special characters.

  ```
  <sysname> system-view
  [sysname] hwatacs-server template template1
  [sysname-hwtacas-template1] hwatacacs-server shared-key cipher key-string
  ```

9. Configure the password policy to set the password strength to high (when changing a password, an EU user has to comply with the requirement).

   ```
   <sysname> system-view
   [sysname] password-policy
   [sysname-password] level high
   ```

10. Enable the module to support strong encryption algorithms.

    ```
    <sysname> system-view
    [sysname] web-manager security cipher-suit high-strength
    ```

11. Configure the Public Key Infrastructure (PKI) security rule.

    # Configure the digest algorithm used to sign certificate enrollment requests to SHA-384.The module always enables the following algorithms for PKI:sha1、sha-256、sha-384 and sha-512. Run the following commands to set your preference.

    ```
    <sysname> system-view
    [sysname] pki realm test
    [sysname-pki-realm-test] enrollment-request signature message-digest-method
    sha-384
    ```

    # To export the RSA key pair, you must set the encryption method to AES.

    ```
    [sysname] pki export rsa-key-pair test pem test.pem aes password password
    ```

NOTE

The password must contain at least 8 characters in at least three of the following types of characters: lower-case letters, upper-case letters, digits, and special characters.

12. If the keychain service is needed and an authentication algorithm is required, run the following command to set the algorithm. By default, no algorithm is configured for a key ID.

```
<sysname> system-view
[sysname] keychain a mode absolute
[sysname-keychain-a] key-id 1
[sysname-keychain-a-keyid-1] algorithm hmac-sha-256
```

After the completion of the above security rules, the module is running in the FIPS 140-2 Approved mode. In order to keep the module running in the FIPS 140-2 Approved mode, do not change the above configuration during operation, and perform the following operation:

1. Regularly check that the following functions are disabled, and the recommended check interval is a week.

Table 9-1 Disabled functions and check mothods

Disabled Function	Check Mothod

Telnet service	Run the **display telnet server status** command. In the command output:
	● If **TELENT IPv4 server** is **ENABLE**, run the **undo telnet server enable** command to disable the Telnet service.
	`<sysname> system-view`
	`[sysname] undo telnet server enable`
	● If **TELENT IPv6 server** is **ENABLE**, run the **undo telnet ipv6 server enable** command to disable the Telnet6 service.
	`<sysname> system-view`
	`[sysname] undo telnet ipv6 server enable`

FTP service	Run the **display ftp-server** command. In the command output, if **FTP server is running** is displayed, run the **undo ftp server enable** command to disable the FTP service.
	`<sysname> system-view`
	`[sysname] undo ftp server enable`

Northbound management interface	1. Run the **display api netconf configuration** command. In the command output, if **Api netconf server is enable** is displayed, run the **undo api netconf enable** command to disable the NETCONF interface.
	`<sysname> system-view`
	`[sysname] api`
	`[sysname-api] undo api netconf enable`
	2. Run the **display api restconf configuration** command. In the command output, if **The Api http server is running** is displayed, run the **undo api http enable** command to disable the HTTP-based RESTCONF interface. If **The Api https server is running** is displayed, run the **undo api https enable** command to disable the HTTPS-based RESTCONF interface.
	`<sysname> system-view`
	`[sysname] api`
	`[sysname-api] undo api http enable`
	`[sysname-api] undo api https enable`

2. If you need to manage the module based on the PKI certificate, before importing the key pair and the certificate into the memory of the module, make sure that the type of the key pair is not DSA, SM2, or RSAn (n<2048).
3. If you need to set the authentication-mode for NTP service, make sure the MD5 algorithem is not used. Thus will lead you to a configuration of HMAC-SHA256 and the

command is "**ntp-service authentication-keyid** ***key-id*** **authentication-mode hmac-sha256 [cipher]** ***password-key***". In FIPS mode, MD5 shall not be used within the NTP service.

4. By default, no authentication mode is set for VRRP backup group on the interface, if you want to do so, the MD5 mode is not suggested in the approved mode. In FIPS mode, MD5 shall not be used within the VRRP service.