Hewlett Packard Enterprise

HPE 6125XLG Blade Switches

FIPS 140-2 Non-Proprietary Security Policy

Security Level 1 Validation

Version 1.09

June 2016

Revision Record

Date	Revision Version	Change Description	Author
2014-03-17	1.00	Initial draft	HPE
2014-06-10	1.01	Updates based on ACTT	HPE
2014-09-05	1.02	Updates based on ACTT 082814	HPE
2014-12-02	1.03	Updates based on Leidos comments	HPE
2015-03-20	1.04	Updates based on CMVP comments	HPE
2016-01-08	1.05	Updates based on 5900CP and 12910 Switch Series evaluation	HPE
2016-03-02	1.06	Changed HMAC MD5 to HMAC-MD5	HPE
2016-03-23	1.07	In table 8, change Triple-DES to DES In Table 9, change the DSA private key size from 2048 to 256 bits.	HPE
2016-05-10	1.08	Removed RSA Key Agreement for Table 7	HPE
2016-06-02	1.09	Add NDRNG to Table 7. Remove Triple-DES from table 6.	HPE

Table of Contents

TABLE OF TABLES

FIPS 140-2 Non-Proprietary Security Policy for the HPE Networking Switches

Keywords: Security Policy, CSP, Roles, Service, Cryptographic Module

List of abbreviations:

Abbreviation	Full spelling
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
CF	Compact Flash
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Data Encryption Standard
DOA	Dead on arrival
FCoE	Fibre Channel over Ethernet
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IRF	Intelligent Resilient Framework
KAT	Known Answer Test
LED	Light Emitting Diode
LPU	Line Processing Unit
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MPU	Main Processing Unit
NIST	National Institute of Standards and Technology
OAA	Open Application Architecture
OAP	Open Application Platform
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SFP	Small Form-Factor Plugable

Abbreviation	Full spelling
SFP+	Enhanced Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SRPU	Switching and routing processor unit
SSL	Secure Sockets Layer
XFP	10 Gigabit Small Form-Factor Pluggable

1 Introduction

This document is a non-proprietary Cryptographic Module Security Policy for the HPE 6125XLG blade switch. The policy describes how the HPE 6125XLG switch meets the requirements of FIPS 140-2. This document also describes how to configure the HPE 6125XLG switch in FIPS 140-2 mode. This document was prepared as part of the FIPS 140-2 Security Level 1 validation.

FIPS 140-2 standard details the U.S. Government requirements for cryptographic security appliances. More information about the standard and validation program is available on the NIST website at csrc.nist.gov/groups/STM/cmvp/.

This document includes the following sections:

- Overview
- Security Appliance Validation Level
- Physical Characteristics and Security Appliance Interfaces
- Roles, Services and Authentication
- Cryptographic Algorithms
- Cryptographic Key Management
- Self-Tests
- Delivery and Operation
- Physical Security Mechanism
- Mitigation of Other Attacks
- Obtaining Documentation and Technical Assistance

2 Overview

The HPE 6125XLG blade switch module is suitable for a range of uses: at the edge of a network, connecting server clusters in a data center, in an enterprise LAN core, and in large-scale industrial networks and campus networks. The switch is based on the Comware Version 7.1.045 platform.

The HPE 6125XLG blade switch module is being validated as a multi-chip embedded module at FIPS 140-2 Security Level 1.

2.1 **Comware Switch Block Level Diagram**

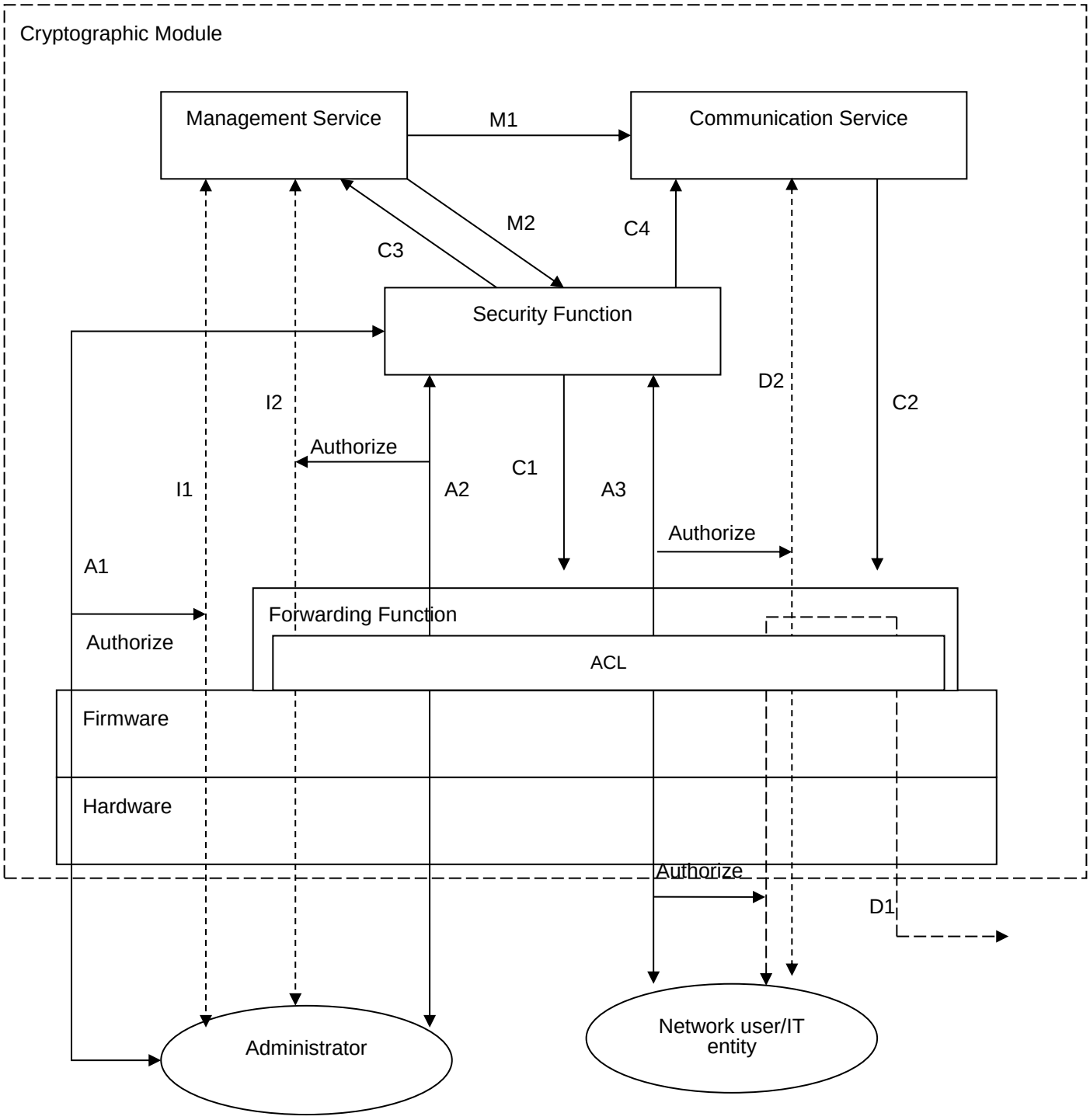

Figure 1 Security Architecture Block Diagram

The cryptographic module provides the following services externally:

1. Management: supports various login methods and configuration interfaces for managing the system.
2. Communication: supports interoperation between the communication protocols at different layers in the protocol stack, such as 802.3, PPP, and IP, and uses the forwarding function to receive/send packets for the local device and forward packets for other devices.

To ensure security, the security function provides appropriate access control for the cryptographic module to identify and authenticate the external entities attempting to access them, and authorize the external entities that pass the identification and authentication. The access control function also records the external entities' accesses to the services, such as the beginning time and end time of a visit. The figure above shows how administrators (crypto officer, user role) and network users access a cryptographic module service.

M2: The administrator accesses the management service to configure the security function.

M1: The administrator accesses the management service to configure the communication service.

C1: The security function issues the forwarding control ACL or other control measures to the forwarding function for security processing like packet filtering.

D2: The communication service uses the forwarding function to receive and send packets for the local device.

C2: The communication service issues routing entries or MAC address entries to the forwarding function for forwarding packets for other devices.

A1: The administrator connects to a physical management interface (the console for example) of the cryptographic module to access the system management access control service of the security function. If the access succeeds, the I1 access to the management service is authorized. The security function uses the C3 authorization action to authorize the administrator administrative roles.

I1: The administrator accesses the management service through the physical management interface.

A2: The administrator connects to a network interface (such as an Ethernet interface) of the cryptographic module to access the system management access control service of the security function. If the access succeeds, the I2 access to the management service is authorized.

I2: The administrator accesses the management service through the network interface.

A3: A network user connects to a network interface of the cryptographic module to access the communication access control service of the security function. If the access succeeds, D1/D2 are authorized. The security function uses the C4 authorization action to authorize the network user the communication service access privilege, namely, the network access privilege.

D1: Forwarding packets for the network user.

To facilitate cryptographic module management, the administrator is allowed to access the system management service by remote login through a network interface. To prevent the authentication data of the administrator (such as the username and password) from being

intercepted and prevent the operation commands from being tampered, the cryptographic module provides the SSH2/HTTPS for secure remote management.

For the management service, the cryptographic module defines predefined roles and custom user roles, which service differs as result of different access permissions.

Each user can switch to a different user role without reconnecting to the device. To switch to a different user role, a user must provide the role switching authentication information. The authentication is role-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

If needed, IPSec can be configured to protect the network data.

No external programs can take control of the cryptographic module, because the cryptographic module does not provide the general-purpose computing service. This ensures the absolute control of the cryptographic module.

2.2 **HPE 6125XLG Switch**

2.2.1 **Product overview**

The HPE 6125XLG Ethernet Blade Switch is the next generation Ethernet blade switch from HPE Networking. Built with the enterprise data center in mind, the HPE 6125XLG is architected to deliver 880G of switching performance for the most demanding applications. The HPE 6125XLG is based on HPE Comware Version 7.1.045 network operating system, which delivers enterprise grade resiliency The 6125XLG is designed for data center convergence with full support for IEEE Data Center Bridging (DCB) for lossless Ethernet, and Fibre Channel over Ethernet (FCoE) protocols. With support for IETF industry standard TRILL (Transparent Interconnection of Lots of Links), the HPE 6125XLG delivers loop free large Layer 2 networks with multi-path support. With HPE's Intelligent Resilient Framework (IRF) multiple switches can be virtualized and managed as a single entity with HPE's Intelligent Management Center (IMC). The HPE 6125XLG is the industry's first blade switch with VEPA (Virtual Ethernet Port Aggregation) support, enabling customers to unify the management of their physical and virtual networks. Combine these features with Virtual Application Network (VAN) and your data center provides the benefits of versatility of a true Virtualized Network. HPE 6125XLG Ethernet Blade Switch provides flexibility, versatility, and resiliency making it the optimal choice for any blade switching environment.

The HPE 6125XLG Ethernet Blade Switch has Four (4) 40 GbE (QSFP+) ports, Eight (8) 10 GbE (SFP+) ports, and 1 Console port to front panel, and 16 10 GbE internal ports to backplane, which connect to each of 16 servers in C7000 Blade System. It also has 4 10GbE cross-connect ports.

2.2.2 **Test Modules**

Testing included one model in the HPE 6125XLG switch:

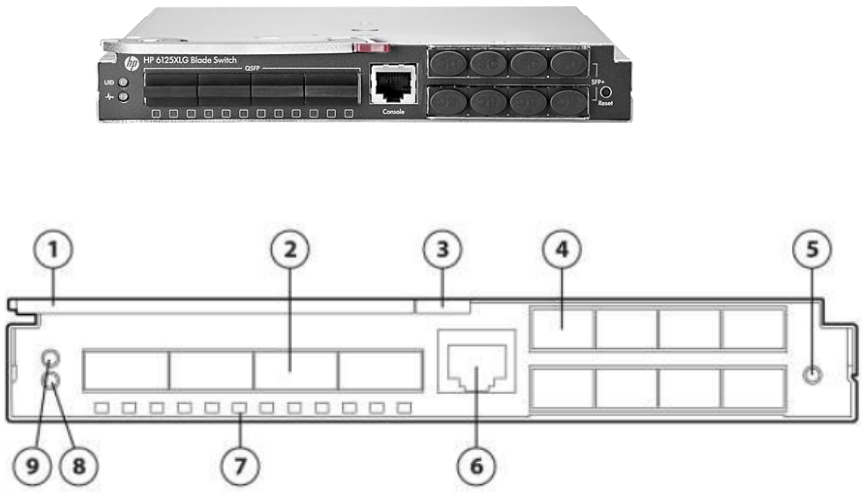

Figure 1 HP 6125XLG Blade Switch

1. Ejector Lever
2. Four (4) 40 GbE (QSFP+) ports
3. Release tab
4. Eight (8) 10 GbE (SFP+) ports
5. Reset button
6. Console port
7. Port LED
8. Health LED
9. Unit ID (UID) LED

Part Number	Module Name
711307-B21	HPE 6125XLG Blade Switch (4 QSFP+ and 8 SFP+ uplink ports, 16 10G KR2 downlink ports, and 4 10G cross-connect ports)

3 Security Appliance Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

Table 1 Validation Level by Section

No.	Area	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
12	Overall Level	1

4 Physical Characteristics and Security Appliance Interfaces

4.1 HPE 6125XLG Switch

The HPE 6125XLG Ethernet Blade Switch is the next generation Ethernet blade switch from HPE Networking. Built with the enterprise data center in mind, the HPE 6125XLG is architected to deliver 880G of switching performance for the most demanding applications. The HPE 6125XLG is based on HPE Comware Version 7.1.045 network operating system, which delivers enterprise grade resiliency The 6125XLG is designed for data center convergence with full support for IEEE Data Center Bridging (DCB) for lossless Ethernet, and Fibre Channel over Ethernet (FCoE) protocols. With support for IETF industry standard TRILL (Transparent Interconnection of Lots of Links), the HPE 6125XLG delivers loop free large Layer 2 networks with multi-path support. With HPE's Intelligent Resilient Framework (IRF) multiple switches can be virtualized and managed as a single entity with HPE's Intelligent Management Center (IMC). The HPE 6125XLG is the industry's first blade switch with VEPA (Virtual Ethernet Port Aggregation) support, enabling customers to unify the management of their physical and virtual networks. Combine these features with Virtual Application Network (VAN) and your data center provides the benefits of versatility of a true Virtualized Network. HPE 6125XLG Ethernet Blade Switch provides flexibility, versatility, and resiliency making it the optimal choice for any blade switching environment.

The HPE 6125XLG Ethernet Blade Switch has Four (4) 40 GbE (QSFP+) ports, Eight (8) 10 GbE (SFP+) ports, and 1 Console port to front panel, and 16 10 GbE internal ports to backplane, which connect to each of 16 servers in C7000 Blade System. It also has 4 10GbE cross-connect ports.

http://h18000.www1.hp.com/products/quickspecs/14612_na/14612_na.pdf describes the ports in detail along with the interpretation of the LEDs.

4.2 Physical Interfaces Mapping

The physical interfaces provided by the HPE Networking products map to four FIPS 140-2 defined logical interface: data input, data output, control input and status output. Table 2 presents the mapping.

Table 2 Correspondence between Physical and Logical Interfaces

Physical Interface	FIPS 140-2 Logical Interface
Networking ports	Data Input Interface
Console port	
Management Ethernet port	
CF card slot	
Networking ports	Data Output Interface

Physical Interface	FIPS 140-2 Logical Interface
Console port	
Management Ethernet port	
CF card slot	
Networking ports	Control Input Interface
Console port	
Management Ethernet port	
Power switches	
Reset Switch	
Port status LED mode switching button	
Networking ports	Status Output Interface
Console port	
Management Ethernet port	
LEDs	
Power Slot	Power Interface
Backplane	

5 Roles, Services, and Authentication

5.1 Roles

The HPE Networking switches provide 18 predefined roles and 64 custom user roles. There are 16 roles (Table 3) in the device that operators may assume:

network-admin, level-15 and security-audit which are the FIPS Crypto-Officer Role,

network-operator, level 0 ~ level 14 and 64 custom user roles which are defined as the FIPS User Role.

Table 3 presents the roles and roles description. The devices allow multiple management users to operate the appliance simultaneously.

The HPE Networking switches do not employ a maintenance interface and do not have a maintenance role.

Table 3 Roles and Role description

FIPS Role	Comware Role Name	Role Description
Crypto-Officer	network-admin	● Accesses all features and resources in the system, except for the display security-logfile summary, info-center security-logfile directory, and security-logfile save commands.
	level-15	Has the same rights as network-admin
	Level-9	Has access to all features and resources except those in the following list. ● RBAC non-debugging commands. ● Local users. ● File management. ● Device management. ● The display history-command all command.
	security-audit	● Security log manager. The user role has the following access to security log files: ● Access to the commands for displaying and maintaining security log files (for example, the dir, display security-logfile summary, and more commands). ● Access to the commands for managing security log files and security log file system (for example, the info-center security-logfile directory, mkdir, and security-logfile save commands). Only the security-audit user role has access to security log files.
User	network-operator	● Accesses the display commands for all features and resources in the system, except for commands such as display history-command all and display security-logfile summary. ● Enables local authentication login users to change their own password.
	level-0	Has access to diagnostic commands, including ping, tracert, and ssh2.
	level-1	Has access to the display commands of all features and resources in the system except display history-command all. The level-1 user role also has all access rights of the user role

		level-0.
	custom user role; level-2 to level-8; level-10 to level-14	Have no access rights by default. Access rights are configurable.

5.2 **Services**

HPE Networking switches provide five services:

- View device status,
- View running status,
- Network functions,
- Security management,
- Configuration function.

You can access these services by using any of the following methods:

- Console Port
- SSH

The console port and SSH present a command line interface while the web user interface is a graphical user interface.

5.2.1 **Crypto Officer Services**

The Crypto Officer role is responsible for the configuration and maintenance of the switches. The Crypto Officer services consist of the following:

Table 4 Crypto officer services

Service	Description	Input	Output	CSP Access	Available to Role
View device status	● View currently running image version; ● View installed hardware components status and version	Commands	Status of devices	None	Network-admin, level-15, level-9
View running status	● View memory status, packet statistics, interface status, current running image version, current configuration, routing table, active sessions, temperature and SNMP MIB statistics.	Commands	Status of device functions	None	Network-admin, level-15, level-9

Perform Network functions	• Network diagnostic service such as “ping”; • Network connection service such as “SSHv2” client; • Provide IKEv1/IPsec service to protect the session between the switch and external server(e.g. Radius Server/Log Server) • Initial Configuration setup (IP, hostname, DNS server)	Commands and configuration data	Status of commands and configuration data	CSP1-1: RSA private keys (read access); CSP1-2: DSA private keys (read access); CSP1-3: Public keys (read access); CSP2-1: IPsec authentication keys(read/write access); CSP2-2: IPsec encryption keys(read/write access); CSP2-3: IKE pre-shared keys(read access); CSP2-4: IKE Authentication key(read/write access); CSP2-5: IKE Encryption Key(read/write access); CSP2-6: IKE RSA Authentication private Key(read access); CSP2-7: IKE DSA Authentication private Key(read access); CSP2-8: IKE Diffie-Hellman Key Pairs(read access); CSP3-1: SSH RSA Private key(read access); CSP3-2: SSH Diffie-Hellman Key Pairs(read/write access); CSP3-3: SSH Session Key(read/write access); CSP3-4: SSH Session authentication Key(read/write access); CSP4-1: User Passwords(read/write access);	Network-admin, level-15, level-9

				CSP4-2: super password(read access); CSP4-3: RADIUS shared secret keys(read access); CSP4-4: TACACS+ shared secret keys(read access); CSP5-1: DRBG entropy input(read/write access); CSP6-1: DRBG seed(read access); CSP6-2: DRBG V(read access); CSP6-3: DRBG Key(read access); CSP7-1: SNMPv3 Authentication Key(read access); CSP7-2: SNMPv3 Encryption Key(read access);	
Perform Security management	● Change the role; ● Reset and change the password of same/lower privilege user; ● Maintenance of the super password; ● Maintenance (create, destroy, import, export) of public key/private key/shared key; ● Maintenance of IPsec/IKE. ● Maintenance of SNMPv3 ● Management (create, delete, modify) of the user roles; ● Management of the access control rules for each role; ● Management (create, delete, modify) of the user account; ● Management	Commands and configuration data	Status of commands and configuration data	CSP1-1: RSA private key(write access); CSP1-2: DSA private key(write access); CSP1-3: Public keys(write access); CSP2-3: IKE pre-shared keys(write access); CSP4-1: User Passwords(write access); CSP4-2: super password(write access); CSP4-3: RADIUS shared secret keys(write access); CSP4-4: TACACS+ shared secret keys(write access); CSP5-1: DRBG entropy input(read access); CSP6-1: DRBG seed(read access);	Network-admin, level-15, level-9, security-audit

	of the time; ● Maintenance (delete, modify) system start-up parameters; ● File operation (e.g. dir, copy, del); ● Shut down or Reboot the security appliance; ● Perform self-test			CSP6-2: DRBG V(read access); CSP6-3: DRBG Key(read access); CSP7-1: SNMPv3 Authentication Key(write access); CSP7-2: SNMPv3 Encryption Key(write access); CSP8-1: System KEK	
Perform Configuration functions	● Save configuration; ● Management of information center; ● Define network interfaces and settings; ● Set the protocols the switches will support(e.g. SFTP server, SSHv2 server); ● Enable interfaces and network services; ● Management of access control scheme ● Shut down or Reboot the security appliance;	Commands and configuration data	Status of commands and configuration data	CSP1-1: RSA private key(write access); CSP1-2: DSA private key(write access); CSP1-3: Public keys(write access); CSP2-3: IKE pre-shared keys(write access); CSP4-1: User Passwords(write access); CSP4-2: super password(write access); CSP4-3: RADIUS shared secret keys(write access); CSP4-4: TACACS+ shared secret keys(write access); CSP7-1: SNMPv3 Authentication Key(write access); CSP7-2: SNMPv3 Encryption Key(write access); CSP8-1: System KEK	Network-admin, level-15, level-9, security-audit

5.2.2 **User Services**

The following table describes the services available to user service.

Table 5 user service

Service	Description	Input	Output	CSP Access	Available to Role

View device status	● View currently running image version; ● View installed hardware components status and version	Commands	Status of devices	None	network-operator
View running status	● View memory status, packet statistics, interface status, current running image version, current configuration, routing table, active sessions, temperature and SNMP MIB statistics.	Commands	Status of device functions	None	network-operator
Perform Network functions	● Network diagnostic service such as “ping”; ● Network connection service such as “SSHv2” client;	Commands and configuration data	Status of commands and configuration data	CSP1-1: RSA private key(read/write access); CSP1-2: DSA private key(read access); CSP1-3: Public keys(read access); CSP2-1: IPsec authentication keys(read/write access); CSP2-2: IPsec encryption keys(read/write access); CSP2-3: IKE pre-shared keys(read access); CSP2-4: IKE Authentication key(read/write access); CSP2-5: IKE Encryption Key(read/write access); CSP2-6: IKE RSA Authentication private Key(read access);	Level-0, Level-1

				CSP2-7: IKE DSA Authentication private Key(read access); CSP2-8: IKE Diffie-Hellman Key Pairs(read access); CSP3-1: SSH RSA Private key(read access); CSP3-2: SSH Diffie-Hellman Key Pairs(read/write access); CSP3-3: SSH Session Key(read/write access); CSP3-4: SSH Session authentication Key(read/write access); CSP4-1: User Passwords(read/write access); CSP4-2: super password(read access); CSP4-3: RADIUS shared secret keys(read access); CSP4-4: TACACS+ shared secret keys(read access); CSP5-1: DRBG entropy input(read/write access); CSP6-1: DRBG seed(read access);	

				CSP6-2: DRBG V(read access); CSP6-3: DRBG Key(read access); CSP7-1: SNMPv3 Authentication Key(read access); CSP7-2: SNMPv3 Encryption Key(read access); CSP8-1: System KEK	

5.2.3 **Unauthenticated Services**

- Cycle the power on the switch
- View currently running image version;
- View installed hardware components status and version
- View memory status, packet statistics, interface status, current running image version, current configuration, routing table, active sessions, temperature and SNMP MIB statistics

5.2.4 **Non-Approved Services**

The HPE network switches supports the following non-approved services:

- Internet Key Exchange (IKE) with DES, MD5, HMAC-MD5, Diffie-Hellman (<2048-bits), RSA (< 2048-bits), DSA (< 2048-bits).
- Perform Network Time Protocol (NTP) service.
- Perform Secure Socket Layer (SSL) version 3.0.
- Perform TLS 1.0 with DES, RC4, MD5, HMAC-MD5, RSA (< 2048-bits).
- Perform Secure Shell version 1.x.
- Perform Secure Shell version 2.0 with DES, MD5, HMAC-MD5, DSA (<2048-bits)
- Perform Telnet

5.3 **Authentication Mechanisms**

HPE networking devices support identity-based authentication, and role-based access control.

- Identity-based authentication

Each user is authenticated upon initial access to the device. The authentication is identity-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

To logon to the appliances, an operator must connect to it through one of the management interfaces (console port, SSH, HTTPS) and provide a password.

A user must be authenticated using usernames and passwords. The minimum password length is 15 characters, and the maximum is 63. The passwords must contain at least one lower case letter (26), one upper case letter (26), one special character (32) and one numeric character (10). The remaining eleven characters can be a lower case letter (26), an upper case letter (26), a special character (32) and/or a numeric character (10) equaling 94 possibilities per character. An alpha, numeric or special character cannot appear three or more times consecutively. Therefore, for a 15 characters password, the probability of randomly guessing the correct sequence is 1 in 64,847,834,440,785 (this calculation is based on the use of the typical standard American QWERTY computer keyboard. The calculation is 26 x 26 x 32 x 10 x 94 x 93 x 94 x 94 x 93 x 94 x 94 x 93 x 94 x 94 x 93 = 64,847,834,440,785. Assuming the first four digits are one from each character set [26 x 26 x 32 x 10] the fifth digit can be from the complete set of available characters [94]. Since a character or number cannot appear three or more times consecutively, for the sixth character the set of available characters is decreased by 1 [93]. The seventh and eighth character again can draw from the complete set of available characters [94 x 94]. Since a character or number cannot appear three or more times consecutively, for the ninth character the set of available characters is decreased by 1 [93]. This pattern continues for the remaining characters in the password.)

In order to guess the password in 1 minute with close to probability 1 requires 64,847,834,440,785 trials, which is stronger than the one in a million chance required by FIPS 140-2. By default, the maximum number of consecutive failed login attempts is three and a user failing to log in after the specified number of attempts must wait for one minute before trying again. Using Anderson's formula to calculate the probability of guessing a password in 1 minute:

- *P* probability of guessing a password in specified period of time
- *G* number of guesses tested in 1 time unit
- *T* number of time units
- *N* number of possible passwords

Then $P >= T \times G / N$ (4.6262E-14 = 1 x 3 / 64,847,834,440,785)

The probability of guessing a password in 1 minute is 4.6262E-14.

To provide additional password security, Comware 7.1 provides additional limits to the number of consecutive failed login attempts. If an FTP or VTY user fails authentication, the system adds the user to a password control blacklist. If a user fails to provide the correct password after the specified number of consecutive attempts, the system can take one of the following actions, based on the administrator's choice:

Blocks the user's login attempts until the user is manually removed from the password control blacklist.

Blocks the user's login attempts within a configurable period of time, and allows the user to log in again after the period of time elapses or the user is removed from the password control blacklist.

HPE Networking devices can also use certificate credentials using 2048 bit RSA keys and SHA-256; in such a case the security strength is 112 bits, so an attacker would have a 1 in 2^112

chance of a successful authentication which is much stronger than the one in a million chance required by FIPS 140-2.

The users who try to log in or switch to a different user privilege level can be authenticated by RADIUS and TACACS+ Server. The minimum password length is 15 characters, and the maximum is 63. Therefore, for a 15 characters password, the probability of randomly guessing the correct sequence is one in 64,847,834,440,785. The device (RADIUS client) and the RADIUS server use a shared key to authenticate RADIUS packets and encrypt user passwords exchanged between them. For more details, see RFC 2865: 3 Packet Format Authenticator field and 5.2 User-password.

- Role-based access control

  In Comware Version 7.1.045, the command and resource access permissions are assigned to roles.

  Users are given permission to access a set of commands and resources based on the users' user roles. Each user can have one or more roles.

6 Cryptographic Algorithms

6.1 FIPS Approved Cryptographic Algorithms

The following table lists the FIPS-Approved algorithms HPE Networking devices provide.

Table 6 FIPS-Approved Cryptography Algorithms

Algorithm	Bits of Security	Application	Certificate
AES-128 AES-192 AES-256	128 192 256	Kernel – Encryption/decryption	#2990
AES-128 AES-192 AES-256	128 192 256	Encryption/decryption	#2943
SHA-1	80	Kernel – Hashing	#2511
SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	80 112 128 192 256	Hashing	#2479
HMAC SHA-1	160	Kernel - Message Authentication	#1896
HMAC SHA-1 HMAC SHA-224 HMAC SHA-256 HMAC SHA-384 HMAC SHA-512	160 224 256 384 512	Message Authentication	#1866
RSA-SHA1	80	Digital Signature Verification	#1546
RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512	112 (RSA-2048)	Key Pair Generation, Digital Signature Generation Digital Signature Verification	#1546
DSA-SHA1	80	Digital Signature Verification	#875
DSA-SHA224 DSA-SHA256 DSA-SHA384 DSA-SHA512	112 (DSA-2048)	Key Pair Generation, Digital Signature Generation Digital Signature Verification	#875

Algorithm	Bits of Security	Application	Certificate
CTR DRBG		Random bits generation	#546
Component Validation List (CVL)		SP800-135 KDF[1] (IKEv1, SSH, SNMP[2])	#341[3]

6.2 FIPS Allowed Cryptographic Algorithms

The following table contains the set of FIPS Allowed cryptographic algorithms that can also be used in FIPS mode.

Table 7 FIPS-Allowed Cryptography Algorithms

Algorithm	Bits of Security	Application
DH 2048	112	Key Agreement
RSA 2048	112	Key Wrapping
NDRNG		entropy gatherer for the DRBG

6.3 Non-FIPS Approved Cryptographic Algorithms

The following table contains the set of non-FIPS Approved algorithms that are implemented but may not be used when operating in FIPS mode. These algorithms are used in non-FIPS mode.

Table 8 Non-FIPS Approved Cryptography Algorithms

Algorithm	Application
DES	Encryption/decryption
Diffie-Hellman (< 2048-bits)	Key Agreement
RC4	Encryption/decryption
MD5	Hashing
HMAC-MD5	Message Authentication
RSA (<2048)	Key Pair Generation, Digital Signature Generation Digital Signature Verification Key Agreement

[1] The KDF (key derivation function) used in each of IKEv1, SSH and SNMP protocols was certified by CAVP with CVL Cert. #341.
[2] These protocols have not been reviewed or tested by the CAVP and CMVP
[3] Although the certification contains TLS, it is not used in this version of Comware.

Algorithm	Application
	Key Wrapping
DSA (<2048)	Key Pair Generation, Digital Signature Generation Digital Signature Verification

7 Cryptographic Key Management

7.1 Cryptographic Security Parameters

The security appliances use a variety of Critical Security Parameters (CSP) during operation. The following table lists the CSP including cryptographic keys used by the HPE Networking devices. It summarizes generation, storage, and zeroization methods for the CSP.

Table 9 Cryptographic Security Parameters

#	Key/ CSP Name	Algorithm	Key Size	Description	Storage	Zeroization
Public key management						
CSP1-1	RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself.	FLASH (cipher text / AES256)	Using CLI command to zeroize.
CSP1-2	DSA private key	DSA	256 bits	Identity certificates for the security appliance itself.	FLASH (cipher text / AES256)	Using CLI command to zeroize
CSP1-3	Public keys	DSA/ RSA	1024 bits ~ 2048 bits	Public keys of peers to validate the digital signature	FLASH(plain text)	Delete public keys of peers from configuration, write to startup config
IPsec						
CSP2-1	IPsec authentication keys	HMAC-SHA1	160 bits	Used to authenticate the IPsec traffic	RAM (plain text)	Automatically when session expires.
CSP2-2	IPsec encryption keys	AES	128 bits 192 bits, 256 bits	Used to encrypt the IPsec traffic	RAM (plain text)	Automatically when session expires.
CSP2-3	IKE pre-shared keys	Shared Secret	6 ~ 128 bytes	Entered by the Crypto-Officer in plain text form and used for authentication during IKE	FLASH(cipher text/ AES-CTR-256) and RAM (cipher text/ AES-CTR-256)	Using CLI command to zeroize
CSP2-4	IKE Authentication key	HMAC-SHA1	160 bits	Used to authenticate IKE negotiations	RAM (plain text)	Automatically when session expires.

#	Key/ CSP Name	Algorithm	Key Size	Description	Storage	Zeroization
CSP2-5	IKE Encryption Key	AES	128 bits 192 bits, 256 bits	Used to encrypt IKE negotiations	RAM (plain text)	Automatically when session expires.
CSP2-6	IKE RSA Authentication private Key	RSA	2048 bits	private key used for IKE protocol during the handshake	RAM(plain text)	Automatically when handshake finishing
CSP2-7	IKE DSA Authentication private Key	DSA	2048 bits	private key used for IKE protocol during the handshake	RAM(plain text)	Automatically when handshake finishing
CSP2-8	IKE Diffie-Hellman Key Pairs	Diffie-Hellman	2048 bits	Key agreement for IKE	RAM (plain text)	Automatically when handshake finishing
SSH						
CSP3-1	SSH RSA Private key	RSA	2048 bits	private key used for SSH protocol	RAM(plain text)	Automatically when handshake finishing
CSP3-2	SSH Diffie-Hellman Key Pairs	Diffie-Hellman	2048 bits	Key agreement for SSH sessions.	RAM (plain text)	Automatically when handshake finishing
CSP3-3	SSH Session Key	AES	128 bits, 256 bits	SSH session symmetric key	RAM (plain text)	Automatically when SSH session terminated
CSP3-4	SSH Session authentication Key	HMAC-SHA1	160 bits	SSH session authentication key	RAM (plain text)	Automatically when SSH session terminated
AAA						
CSP4-1	Crypto-Officer Password	Secret	15 ~ 63 bytes	Used to authenticate the administrator role.	FLASH (cipher text / AES256)	Using CLI command to zeroize
CSP4-2	User Password	Secret	15 ~ 63 bytes	Used to authenticate the user role.	FLASH (cipher text / AES256)	Using CLI command to zeroize

#	Key/ CSP Name	Algorithm	Key Size	Description	Storage	Zeroization
CSP4-3	RADIUS shared secret keys	Shared Secret	15 ~ 64 bytes	Used for authenticating the RADIUS server to the security appliance and vice versa.	FLASH (cipher text / AES256)	Using CLI command to zeroize
CSP4-4	TACACS+ shared secret keys	Shared Secret	15~255 bytes	Used for authenticating the TACACS+ server to the security appliance and vice versa.	FLASH (cipher text / AES256)	Using CLI command to zeroize
Entropy						
CSP5-1	DRBG entropy input	SP 800‐90 CTR_DRBG	256 bits	Entropy source used to construct seed	RAM (plaintext)	Resetting or rebooting the security appliance
Random Bits Generation						
CSP6-1	DRBG seed	SP 800‐90 CTR_DRBG	384 bits	Input to the DRBG that determines the internal state of the DRBG	RAM (plaintext)	Resetting or rebooting the security appliance
CSP6-2	DRBG V	SP 800‐90 CTR_DRBG	128 bits	Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	RAM (plaintext)	Resetting or rebooting the security appliance
CSP6-3	DRBG Key	SP 800‐90 CTR_DRBG	256 bits	DRBG key used for SP 800-90 CTR_DRBG	RAM (plaintext)	Resetting or rebooting the security appliance
SNMPv3						
CSP7-1	SNMPv3 Authentication Key	SHA1	160 bits	Used to verify SNMPv3 packet.	FLASH (cipher text / AES256) RAM (plain text)	Using CLI command to zeroize

#	Key/ CSP Name	Algorithm	Key Size	Description	Storage	Zeroization
CSP7-2	SNMPv3 Encryption Key	AES	128 bits	Used to encrypt SNMPv3 packet.	FLASH (cipher text / AES256) RAM (plain text)	Using CLI command to zeroize
System KEK						
CSP8-1	Key encrypting key	AES	256 bits	Used to encrypt all private key, user password, and pre-shared key stored on internal storage. The KEK is generated using random bytes	RAM(plain text)	Zeroized when Resetting or rebooting the security appliance

7.2 **Access Control Policy**

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed below. The types of access are: read (r), write (w), and delete (d).

Table 10 Access by Service for Crypto Officer

Service Access /CSP	Network functions	Security management	Configuration functions
PKI			
CSP1-1	r	wd	wd
CSP1-2	r	wd	wd
CSP1-3	r	wd	wd
IPsec			
CSP2-1	rwd	d	
CSP2-2	rwd	d	
CSP2-3	r	wd	wd
CSP2-4	rwd	d	
CSP2-5	rwd	d	
CSP2-6	rd	d	
CSP2-7	rd	d	
CSP2-8	rd	d	

Service Access /CSP	Network functions	Security management	Configuration functions
SSH			
CSP3-1	rd	d	
CSP3-2	rwd	d	
CSP3-3	rwd	d	
CSP3-4	rwd	d	
AAA			
CSP4-1	rwd	wd	wd
CSP4-2	r	wd	wd
CSP4-3	r	wd	wd
CSP4-4	r	wd	wd
Entropy			
CSP5-1	rw	r	
Random Bits Generation			
CSP6-1	r	r	
CSP6-2	r	r	
CSP6-3	r	r	
SNMPv3			
CSP7-1	r	wd	wd
CSP7-2	r	wd	Wd
System KEK			
CSP8-1	r	r	r

Table 11 Access by Service for User role

Service Access /CSP	Network functions	Configuration functions
Public key management		
CSP1-1	r	
CSP1-2	r	
CSP1-3	r	

Service Access /CSP	Network functions	Configuration functions
IPsec		
CSP2-1	rwd	
CSP2-2	rwd	
CSP2-3	r	
CSP2-4	rwd	
CSP2-5	rwd	
CSP2-6	rd	
CSP2-7	rd	
CSP2-8	rd	
SSH		
CSP3-1	rd	
CSP3-2	rwd	
CSP3-3	rwd	
CSP3-4	rwd	
AAA		
CSP4-1	rwd	
CSP4-2	r	
CSP4-3	r	
CSP4-4	r	
Entropy		
CSP5-1	rw	
Random Bits Generation		
CSP6-1	r	
CSP6-2	r	
CSP6-3	r	
SNMPv3		
CSP7-1	r	
CSP7-2	r	
System KEK		

Service Access /CSP	Network functions	Configuration functions
CSP8-1	r	r

8 Self-Tests

HPE Networking devices include an array of self-tests that are run during startup and during operations to prevent any secure data from being released and to insure all components are functioning correctly.

8.1 Power-On Self-Tests

The following table lists the power-on self-tests implemented by the switches. The switches perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any role can perform services. The power-on self-tests are performed prior to the initialization of the forwarding function, which prevents the security appliance from passing any data during a power-on self-test failure.

Table 12 Power-On Self-Tests

Implementation	Tests Performed
Security Appliance Software	Firmware Test (non-Approved RSA 2048 with SHA-256 which acts as a 256 bit EDC)
	DSA signature and DSA verification PWCT
	RSA signature and RSA verification KAT
	RSA signature and RSA verification PWCT
	RSA encryption and RSA decryption PWCT
	Kernel AES encryption and AES decryption KAT
	AES encryption and AES decryption KAT
	Kernel SHA-1 KAT
	SHA-1 KAT
	SHA224 KAT
	SHA256 KAT
	SHA384 KAT
	SHA 512 KAT
	Kernel HMAC SHA-1 KAT
	HMAC SHA-1 KAT
	HMAC SHA224 KAT
	HMAC SHA256 KAT
	HMAC SHA384 KAT
	HMAC SHA 512 KAT

Implementation	Tests Performed
	SP800-90a CTR_DRBG KATs (Instantiate KAT, Generate KAT and Reseed KAT)

8.2 Conditional Self-Tests

The following table lists the conditional self-tests implemented by the switches. Conditional self-tests run when a switch generates a DSA or RSA key pair and when it generates a random number.

Table 13 Conditional Self-Tests

Implementation	Tests Performed
Security Appliance Software	Pairwise consistency test for RSA
	Pairwise consistency test for DSA
	Continuous Random Number Generator Test for the FIPS-approved SP800-90a CTR_DRBG
	Continuous Random Number Generator Test for entropy source (NDRNG)
	Firmware Load Test (RSA PKCS#1 v1.5 2048 bits with SHA-256)

9 Delivery and Operation

9.1 Secure Delivery

To ensure no one has tampered with the goods during delivery, inspect the Networking switch physical package and check as follows:

1. Outer Package Inspection
    1) Check that the outer carton is in good condition.
    2) Check the package for a HPE Quality Seal or IPQC Seal, and ensure that it is intact.
    3) Check that the IPQC seal on the plastic bag inside the carton is intact.
    4) If any check failed, the goods shall be treated as dead-on-arrival (DOA) goods.
2. Packing List Verification

    Check against the packing list for discrepancy in material type and quantity. If any discrepancy found, the goods shall be treated as DOA goods.

3. External Visual Inspection

    Inspect the cabinet or chassis for any defects, loose connections, damages, and illegible marks. If any surface defect or material shortage found, the goods shall be treated as DOA goods.

4. Confirm Software/firmware
    1) Version verification

        To verify the software version, start the appliance, view the self-test result during startup, and use the display version command to check that the software version is “HPE Comware Software, Version 7.1.045, Release 2406” indicates it is a FIPS 140-2 and CC certification version. If software loading failed or the version information is incorrect, please contact HPE for support.

    2) RSA w/ SHA-256 verification

        To verify that software/firmware has not been tampered, run SHA Hash command on the appliance. If the hash value is different from release notes of this software, contact HPE for support. To get release notes, please access HPE website.

5. DOA (Dead on Arrival)

    If the package is damaged, any label/seal is incorrect or tampered, stop unpacking the goods, retain the package, and report to HPE for further investigation. The damaged goods will be replaced if necessary.

9.2 Secure Operation

The rules for securely operating an HPE Networking switch in FIPS mode are:

1. Install and connect the device according to the installation and configuration guides.

2. Start the device, and enter the configuration interface.
3. Check and configure the clock.
4. By default, the device does not run in FIPS mode. Enable the device to work in FIPS mode using the **fips mode enable** command in system view. This will allow the switch to internally enforce FIPS-compliance behavior, such as run power-up self-test and conditional self-test.
5. Set up username/password for crypto officer role. The password must comprise no less than 15 characters and must contain uppercase and lowercase letters, digits, and special characters. By default, the maximum number of consecutive failed login attempts is three and a user failing to log in after the specified number of attempts must wait for one minute before trying again. Verify this is the minimum setting.
6. Save the configurations and re-start the device.

The device works in FIPS mode after restarting:

1. Configure the security appliance to use SSHv2.

An operator can determine whether a switch is in FIPS mode with the command **display fips status**. When in FIPS mode:

1. The FTP/TFTP server is disabled.
2. The Telnet server is disabled.
3. The HTTP server is disabled.
4. SNMP v1 and SNMP v2c are disabled. Only SNMP v3 is available.
5. The SSH server does not support SSHv1 clients
6. Generated RSA/DSA key pairs have a modulus length 2048 bits.
7. SSH, SNMPv3, IPsec and SSL do not support Non-FIPS approved cryptographic algorithms.

10 Physical Security

The HPE 6125XLG Blade Module conforms to the Level 1 requirements for physical security. The hardware portion of the cryptographic module is a production grade component. All internal hardware, firmware, and cryptographic data are protected by the enclosure of the module, which makes up its physical cryptographic boundary. The cryptographic module must be used in a production grade enclosure.

11 Mitigation of Other Attacks

The Security appliances do not claim to mitigate any attacks in a FIPS approved mode of operation.

12 Documentation References

12.1 Obtaining documentation

You can access the HPE Networking products page: http://h17007.www1.hp.com/us/en/ , where you can obtain the up-to-date documents of HPE Routers and Switches, such as datasheet, installation manual, configuration guide, command reference, and so on.

12.2 Technical support

For technical or sales related question please refer to the contacts list on the HPE website: http://www.HPE.com.

The actual support website is:

http://www8.hp.com/us/en/support-drivers.html