CHECK POINT™
YOU DESERVE THE BEST SECURITY

Check Point Software Technologies

Quantum Security Gateway Cryptographic Library

Version 1.1 (Firmware)

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Document revision 046, August 2023

Prepared for Check Point
Software Technologies Ltd. by

Check Point Software Technologies
5 Shlomo Kaplan
Tel Aviv, 6789159
Israel
http://www.checkpoint.com/

RYCOMBE
CONSULTING

Rycombe Consulting Limited
http://www.rycombe.com
+44 7780 682240

Contents

Figures

1 Introduction

This section identifies the cryptographic module; describes the purpose of this document; provides external references for more information; and explains how the document is organized.

1.1 Identification

Module Name	Quantum Security Gateway Cryptographic Library
Module Version	1.1

1.2 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the Quantum Security Gateway Cryptographic Library, also referred to as “the module” within this document. This Security Policy details the secure operation of Quantum Security Gateway Cryptographic Library as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.3 References

For more information on Check Point products please visit: http://www.checkpoint.com/. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission documentation may be Check Point proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Check Point.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

1.5 Document Terminology

Term	Description
AES	Advanced Encryption Standard
AH	Authentication Header
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input Output Services
CAVP	Cryptographic Algorithm Validation Program
CMAC	Cipher-based Message Authentication Code
CMSP	Cryptographic Module Security Policy
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit (Microprocessor)
CSP	Critical Security Parameters
DES	Data Encryption Standard
DRBG	Deterministic Random-bit Generator
DVD	Digital Video Disc
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
ESX	Elastic Sky X: An enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers
FIPS	Federal Information Processing Standard
GAiA	Check Point proprietary operating environment
HDD	Hard Disk Drive
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange
IPsec	Internet Protocol Security: a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session
KDF	Key Derivation Function
LCD	Liquid Crystal Display
LED	Light Emitting Diode
N/A	Not Applicable
NDRNG	Non-deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OS	Operating System
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
RAM	Random-access Memory
RBG	Random Bit Generator
RFC	Request for Comments

TERM	DESCRIPTION
RNG	Random Number Generator
RSA	An algorithm for public-key cryptography. Named after Rivest, Shamir and Adleman who first publicly described it.
SATA	Serial AT Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIC	Secure Internal Communication – a Check Point proprietary protocol
SP	NIST Special Publication document
TLS	Transport Layer Security
Triple-DES	Triple-DES
USB	Universal Serial Bus
VM	Virtual Machine

Figure 1 Document terminology

2 Quantum Security Gateway Cryptographic Library

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

The module provides cryptographic services to Check Point products.

2.2 Module Specification

The Quantum Security Gateway Cryptographic Library is a firmware module that provides cryptographic services to Check Point products.

The module is classified as a multi-chip standalone module.

The module provides a number of NIST validated cryptographic algorithms for services such as IPsec. The module provides applications with a library interface that enables them to access the various cryptographic algorithm functions supplied by the module.

2.2.1 Hardware and Firmware components

The module is a firmware module that resides on either proprietary hardware (see Figure 5) or as a Virtual Machine. For the purposes of FIPS 140-2 testing, the module is validated running with R80.30 firmware on either the Check Point 16200 Plus appliance, the Check Point 28000 appliance, or as a Virtual Machine on HPE DL360 gen 10 running ESXi (see Figure 6) R81.10.05 firmware running on either the Check Point 1530/1535, 1550/1555 and 1570R/1575R Appliances, Check Point 1570/1575 and 1590/1595 Appliances, the Check Point 1600/1800 Appliance, and R81.10 firmware running on the Check Point 3600 appliance or the Check Point 7000 appliance.

The module is packaged as a number of distinct binary images:

File name	Identification for Enterprise Appliances (R80.30)	Identification for SP build (R80.30)	Identification for Enterprise Appliances (R81.10)
libcpbcrypt.so	Build Number = 993000005 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000012 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000011 Major Release = NGX Minor Release = R81_10_jumbo_hf_main
libcpcert.so	Build Number = 993000005 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000012 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000011 Major Release = NGX Minor Release = R81_10_jumbo_hf_main
libcpprng.so	Build Number = 993000005 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000012 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000250 Major Release = NGX Minor Release = ignis_main

File name	Identification for Enterprise Appliances (R80.30)	Identification for SP build (R80.30)	Identification for Enterprise Appliances (R81.10)
libcpopenssl.so	Build Number = 993000002 Major Release = NGX Minor Release = gogo_heat_188_main	Build Number = 993000002 Major Release = NGX Minor Release = gogo_heat_188_main	Build Number = 996000011 Major Release = NGX Minor Release = R81_10_jumbo_hf_main
Vpnd	Build Number = 993000006 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000011 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000011 Major Release = NGX Minor Release = R81_10_jumbo_hf_main
fw_kern_64_3_10_64.o	Build Number = 993000004 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000008 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000027 Major Release = NGX Minor Release = R81_10_jumbo_hf_main
libikev2.so	Build Number = 993000001 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000001 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000008 Major Release = NGX Minor Release = R81_10_jumbo_hf_main
libcptls.so	Build Number = 993000005 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_main	Build Number = 993000012 Major Release = NGX Minor Release = R80_30_JHF_T155_FIPS_FKF_SP_main	Build Number = 996000011 Major Release = NGX Minor Release = R81_10_jumbo_hf_main

Figure 2 Module binary images (Intel processors)

File name	Identification for 1530/1535, 1550/1555 and 1570R/1575R Appliances, Check Point 1570/1575 and 1590/1595 Appliances (R81.10.05)	Identification for 1600/1800 Appliances (R81.10.05)
fw (contains code for libcpbcrypt.so, libcpcert.so, libcpprng.so, Vpnd, libikev2.so, and libcptls.so)	Build Number = 996001220 Major Release = NGX Minor Release = sev_alb_jumbo_hf	Build Number = 996001220 Major Release = NGX Minor Release = sev_alb_jumbo_hf
libcpopenssl.so	Build Number = 996000601 Major Release = NGX Minor Release = sev_alb	Build Number = 996000601 Major Release = NGX Minor Release = sev_alb
fw.o	Build Number = 996001212 Major Release = NGX Minor Release = sev_alb_jumbo_hf	Build Number = 996001212 Major Release = NGX Minor Release = sev_alb_jumbo_hf

Figure 3 Module binary images (Marvell processors)

2.2.2 Cryptographic Boundary

The physical boundary of the module is the case of the hardware appliance on which it is installed. For the purposes of this validation, the module was tested with R80.30 firmware on the Check Point 16200 Plus appliance, the Check Point 28000 appliance and the HPE DL360 gen 10 running ESXi and R81.10.05 firmware running on the Check Point 1530/1535, 1550/1555 and 1570R/1575R Appliances, Check Point 1570/1575 and 1590/1595 Appliances, and the Check Point 1600/1800 Appliance, and R81.10 firmware running on the Check Point 3600 appliance and the Check Point 7000 appliance.

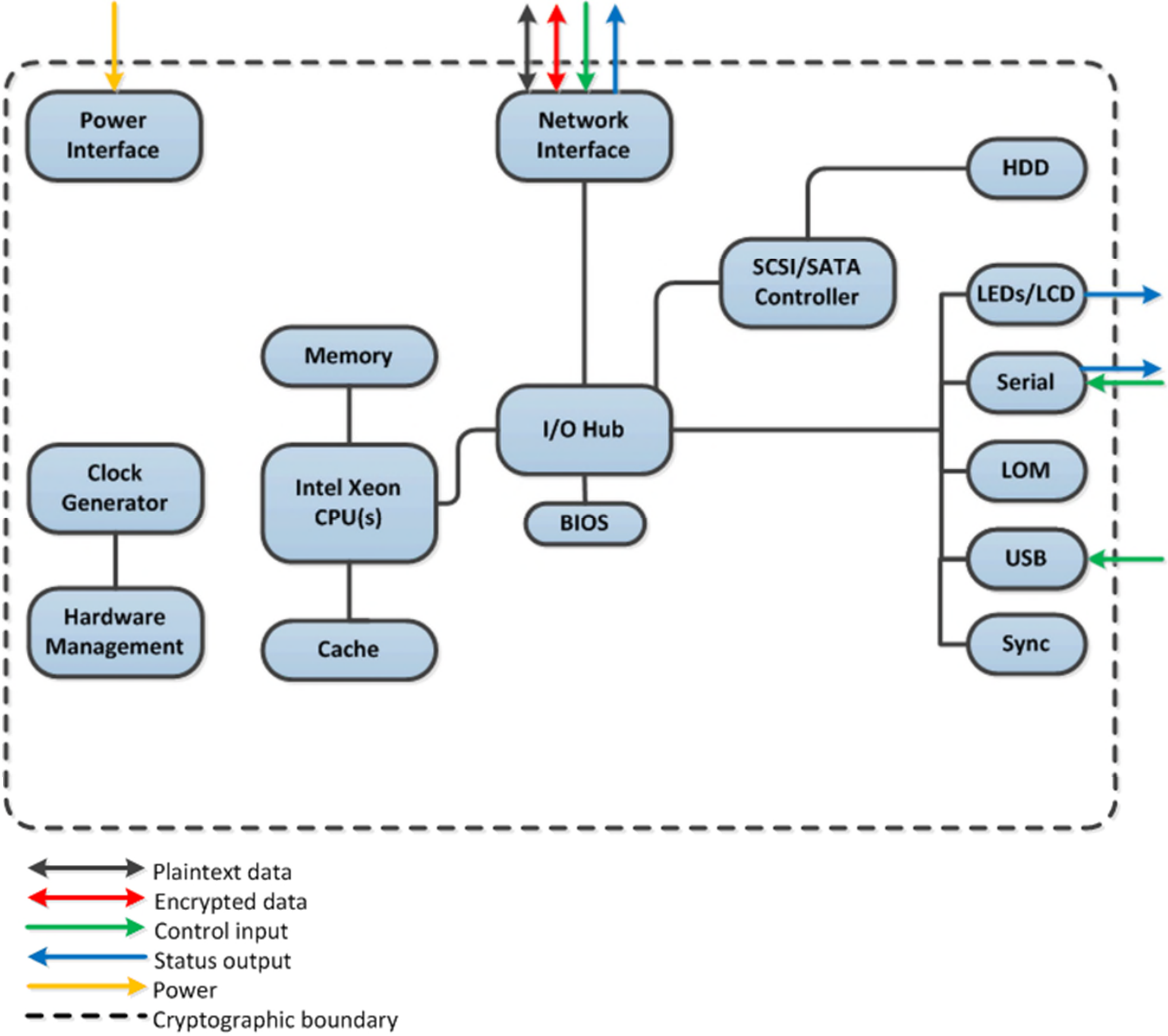

Figure 4 **Block diagram for Check Point 1530/1535/1550/1555/1570/1570R/1575/1575R/1590/1595/1600/1800/3600/7000/16200 Plus/28000 appliance hardware and HPE DL360 gen 10**

The module is a firmware module running on a proprietary hardware platform. See Figure **4**. The processor of this platform executes all firmware. All firmware components of the module are persistently stored within the device and, while executing, are stored in the device local RAM. The cryptographic boundary of the module includes only the module firmware as listed in Figure 2.

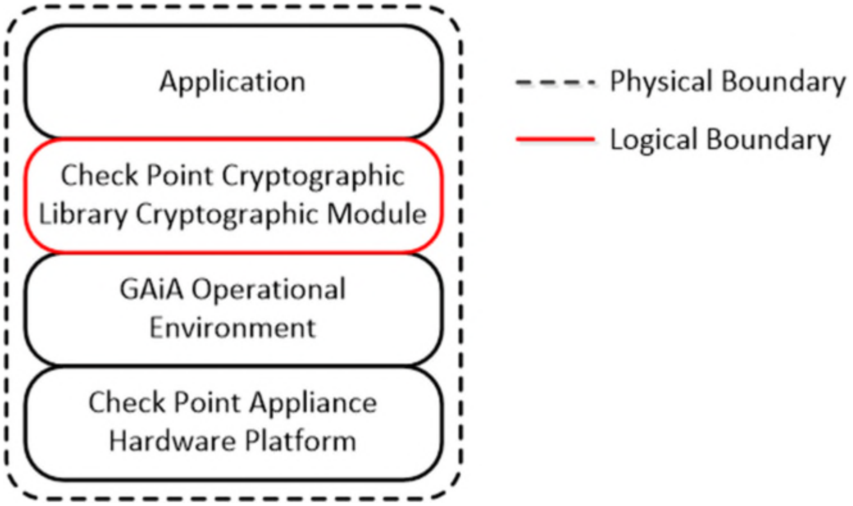
Application
Check Point Cryptographic Library Cryptographic Module
GAiA Operational Environment
Check Point Appliance Hardware Platform
Physical Boundary
Logical Boundary

Figure 5 Logical Diagram of the Cryptographic Boundary with 1530/1535/1550/1555/1570/1570R/1575/1575R/1590/1595/1600/1800/3600/7000/16200 Plus/28000 hardware appliance

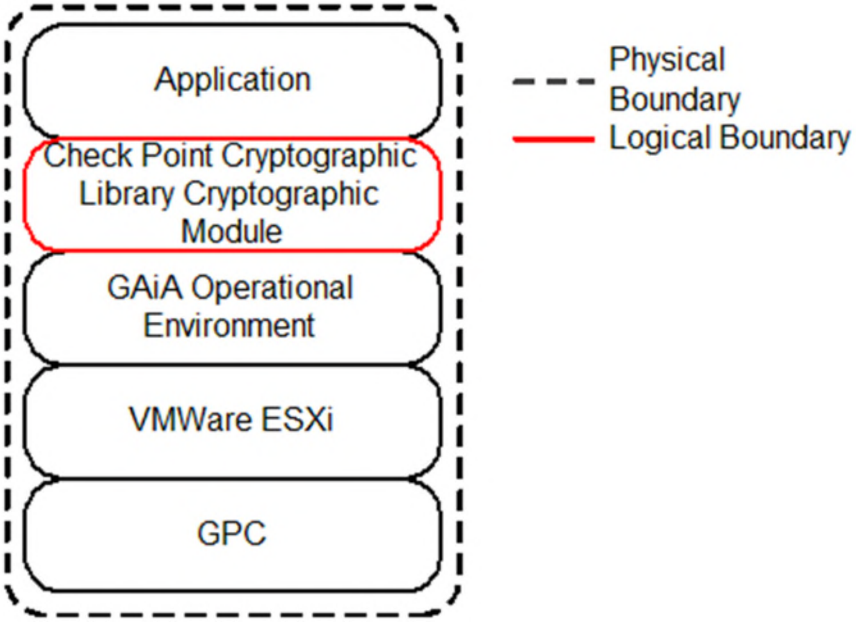
Application
Check Point Cryptographic Library Cryptographic Module
GAiA Operational Environment
VMWare ESXi
GPC
Physical Boundary
Logical Boundary

Figure 6 Logical Diagram of the Cryptographic Boundary with the Cryptographic Module running on a Virtual Machine

2.2.3 Scope of Validation

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Figure 7 Security Level specification per individual areas of FIPS 140-2

2.2.4 Cryptographic Algorithms

2.2.4.1 Approved algorithms

The following table provides details of the approved algorithms that are included within the module:

ALGORITHM TYPE	ALGORITHM	CAVP CERTIFICATE NUMBER	NOTES
Symmetric key	AES	#3418 #A4283	AES with 128-bit or 256-bit keys using CBC and GCM[1][2][3] modes. The modes and sizes are validated for both encryption and decryption.
Asymmetric Key	RSA	#1750 #A4283	Key generation (2048–bit keys). Signature generation (2048-bit/3072-bit with either SHA-256, SHA-384 or SHA-512). Signature verification. (1024-bit/2048-bit signature verification with either SHA-1, SHA-256, SHA-384 or SHA-512).
	ECDSA	#685 #A4283	Supports P-256, P-384, and P-521 curves. FIPS186-4: PKG: CURVES(P-256 P-384 P-521 Testing Candidates) PKV: CURVES(P-256 P-384 P-521) SigGen: CURVES(P-256: (SHA-256) P-384: (SHA-384) P-521: (SHA-512) SigVer: CURVES(P-256: (SHA-256) P-384: (SHA-384) P-521: (SHA-512))
Hashing	SHS	#2824 #A4283	SHA-1[4], SHA-256, SHA-384, SHA-512.

[1] The module complies with SP 800-52 Rev2 and is compatible with the specified versions of TLS in Section 4 of RFC 5288.
The module complies with RFC 6071 and RFC 4106 and that an IKEv2 protocol (RFC 7296) shall be used to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The module also complies with RFC 5282 for authenticated encryption of the encrypted payload of the IKEv2 protocol.

[2] Once the counter portion of the IV reaches its maximum value of 2^32-1, the module aborts the session.

[3] In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

[4] SHA-1 for non-digital signature applications:
SHA-1 is not allowed for digital signature generation. For all other hash function applications, the use of SHA-1 is acceptable. The other applications include HMAC, Key Derivation Functions (KDFs), and hash-only applications (e.g., hashing passwords and using SHA-1 to compute a checksum, such as the approved integrity technique specified in Section 4.6.1 of [FIPS 140-2]).

ALGORITHM TYPE	ALGORITHM	CAVP CERTIFICATE NUMBER	NOTES
Message Authentication Code	HMAC	#2176 #A4283	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512.
Random number generator	Hash DRBG	#823 #A4283	Hash DRBG with SHA-256 and a seed length of 440 bits in accordance with SP800-90A.
Key Agreement	KAS-ECC-SSC	Vendor Affirmed	SP 800-56A rev3 for IPsec and TLS.

Figure 8 Approved Algorithms

The following table lists the key derivation functions (and their associated CVL certificate numbers) implemented by the module.

APPROVED KDF	CAVP CVL CERTIFICATE NUMBER
Transport Layer Security (TLS) v1.0/1.1, v1.2 (SP 800-135 Rev1)	#514 #A4283
Internet Key Exchange (IKE) v1 and v2 (SP 800-135 Rev1)	#514 #A4283

Figure 9 Approved Key Derivation Functions

For each of these approved Key Derivation Functions the module supports or uses the corresponding protocol. These protocols have not been reviewed or tested by the CAVP or CMVP as testing such protocols is not within the scope of CMVP or CAVP activities.

2.2.4.2 Algorithms allowed in approved mode

- RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength).
- The NDRNG that is used to seed the random number generator.

2.2.4.3 Non-approved algorithms

SHA-1 for digital signature generation, any Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 128 bits of encryption strength) variants that are not SP 800-56A rev3 compliant and Triple-DES are available when the module is installed as described in section 3. However, using any of these algorithms results in a non-approved mode of operation.

2.2.5 Components excluded from the security requirements of the standard

There are no components excluded from the security requirements of the standard.

2.3 Physical ports and logical interfaces

The module's physical boundary is that of the device on which it is installed. The device supports sufficient interfaces to allow operators to initiate cryptographic operations and determine the module status.

The module provides its logical interfaces via Application Programming Interface (API) calls. This logical interface exposes services (described in section 2.4.2) that applications utilize directly.

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

FIPS 140-2 Logical Interface	Module Mapping	Appliance/Hardware Physical Interface
Data Input	Parameters passed to the module via API calls	Network ports
Data Output	Data returned from the module via API calls	Network ports
Control Input	API Calls and/or parameters passed to API calls	USB ports, serial console, network ports, power switch
Status Output	Information received in response to API calls	Network ports, serial console, VGA video port, LEDs.
Power Interface	There is no separate power or maintenance access interface beyond the power interface provided by the device that contains the module	Power connector

Figure 10 Module Interfaces

2.4 Roles, Services and Authentication

2.4.1 Roles

The Cryptographic Module implements both a Crypto Officer role and a User role. Roles are assumed implicitly upon accessing the associated services. Section 2.4.2 summarizes the services available to each role.

Role	Description
Crypto Officer	The administrator of the module having full configuration and key management privileges.
User	General User of the module

Figure 11 Roles

2.4.2 Services

Most of the services provided by the module are provided via access to API calls using interfaces exposed by the module.

However, some of the services, such as power-up module integrity testing are performed automatically and so have no function API, but do provide status output.

SERVICE	ROLE	INPUT	OUTPUT	CSP ACCESS	DESCRIPTION
Symmetric Data Encryption and Decryption for IKE/IPsec	User	ESP data.	ESP data.	Session keys.	The module supports IPsec/ESP for data encryption and IPsec/ESP for data integrity.
Symmetric Data Encryption and Decryption for SIC	User	TLS traffic data.	TLS traffic data.	Session keys.	The module supports TLS for data encryption.
Message Digest	User	Data.	Hash of input data.	None.	Used for data packet integrity within ESP and AH. Used by keyed hash and key generation services. This service provides access to SHA-1, SHA-256, SHA-384 and SHA-512 functionality. SHA-1 is non-approved for digital signature generation.
Keyed Hash	User	Data or message.	Keyed hash of input.	HMAC key.	Used for data packet integrity within ESP and AH.
Digital Signature Generation[5]	User	Data.	Digital signature of data.	Asymmetric key pair (read access)	Used to authenticate to the module during IKE.
Digital Signature Verification	User	Signed data.	Result of verification: Success or failure.	Asymmetric key pair (read access)	Used to authenticate to the module during IKE.
RSA Key Generation	Crypto Officer	Size of key required.	Validated RSA key pair.	Asymmetric key pair	Used to generate RSA key pairs.
ECDSA Key Generation	Crypto Officer	Curve	Validated ECDSA key pair.	Asymmetric key pair	Used to generate ECDSA key pairs.
Symmetric Key Generation	Crypto Officer	Size of key required.	Symmetric key	SP 800-90A Hash_DRBG V & C values. Write access: Session keys; Diffie-Hellman key pairs.	Used to generate symmetric key pairs.
Show Status	User/Crypto Officer	Service inputs.	Service outputs.	All CSPs.	The output indicators described for all services. The Show Status service is provided collectively across all services. Each service provides some status information as part of its service output.

[5] The Digital Signature Generation service can be evoked in a non-approved way if SHA-1 is used. See section 3.2 for more details.

SERVICE	ROLE	INPUT	OUTPUT	CSP ACCESS	DESCRIPTION
Self-tests	User	Power up the system or power cycle the system.	Success: Module powers up without error.	Integrity Check key.	Self-tests run automatically at power up. Includes KATs for all approved algorithms and ECDSA P-521 integrity check with SHA-512 for integrity testing of the cryptographic module firmware.

Figure 12 Approved Services

2.4.3 Authentication

The module does not support any authentication mechanisms. The module does not perform authentication.

2.5 Physical Security

The Cryptographic Module is a firmware-only cryptographic module. The module was tested separately on the Check Point 1530/1535, 1550/1555 and 1570R/1575R Appliances, Check Point 1570/1575 and 1590/1595 Appliances, the Check Point 1600/1800 Appliance, the Check Point 3600 appliance, the Check Point 7000 appliance, the Check Point 16200 Plus appliance, the Check Point 28000 appliance and the HPE DL360 gen 10, all of which are built from production-grade components that incorporate standard passivation.

2.6 Operational Environment

The module does not provide a general-purpose operating system (OS) to module operators. The module's operational environment includes Check Point's proprietary non-modifiable GAiA Operating System.

The Quantum Security Gateway Cryptographic Library has been validated on the following operational environments for the purpose of testing:

- Check Point 16200 Plus (previously sold as 16000 turbo) appliance (2nd Gen Intel® Xeon® Silver) with Check Point GAiA Operating System at version R80.30
- Check Point 28000 (previously sold as 26000 turbo) appliance (2nd Gen Intel® Xeon® Gold) with Check Point GAiA Operating System at version R80.30SP
- Check Point GAiA Operating System at version R80.30 on VMware ESXi running on an HPE DL360 gen 10 server (2nd Gen Intel® Xeon® Silver)
- Check Point 3600 appliance (Intel® Atom® C series) with Check Point GAiA Operating System at version R81.10
- Check Point 7000 appliance (2nd Gen Intel® Xeon® Silver) with Check Point GAiA Operating System at version R81.10
- Check Point 1530/1535, 1550/1555 and 1570R/1575R appliances (Marvell® ARMADA® 7K) with Check Point Embedded GAiA Operating System at version R81.10.05

- Check Point 1570/1575 and 1590/1595 appliances (Marvell® ARMADA® 8K) with Check Point Embedded GAiA Operating System at version R81.10.05
- Check Point 1600 and 1800 appliances (Marvell® OCTEON® TX2®) with Check Point Embedded GAiA Operating System at version R81.10.05

The Cryptographic Module is characterized as a firmware module.

The module is also capable of running on the following platforms but has not been tested during this evaluation and no compliance is being claimed on these platforms. Check Point recommends use of the latest Jumbo Hot Fix available:

- Check Point 16200 Plus (previously sold as 16000 turbo) appliance (2nd Gen Intel® Xeon® Silver) with Check Point GAiA Operating System at version R80.40 with Jumbo HF Take_139
- Check Point 16200 Plus (previously sold as 16000 turbo) appliance (2nd Gen Intel® Xeon® Silver) with Check Point GAiA Operating System at version R81 with Jumbo HF Take_72
- Check Point 16200 Plus (previously sold as 16000 turbo) appliance (2nd Gen Intel® Xeon® Silver) with Check Point GAiA Operating System at version R81.10 with Jumbo HF Take_75
- Check Point GAiA Operating System at version R80.40 with Jumbo HF Take_180 on VMware ESXi running on an HPE DL360 gen 10 server (2nd Gen Intel® Xeon® Silver)
- Check Point GAiA Operating System at version R81 with Jumbo HF Take_72 on VMware ESXi running on an HPE DL360 gen 10 server (2nd Gen Intel® Xeon® Silver)
- Check Point GAiA Operating System at version R81.10 with Jumbo HF Take_75 on VMware ESXi running on an HPE DL360 gen 10 server (2nd Gen Intel® Xeon® Silver)
- Check Point 28000 (previously sold as 26000 turbo) appliance (2nd Gen Intel® Xeon® Gold) with Check Point GAiA Operating System at version R81 with Jumbo HF Take_72
- Check Point 28000 (previously sold as 26000 turbo) appliance (2nd Gen Intel® Xeon® Gold) with Check Point GAiA Operating System at version R81.10 with Jumbo HF Take_75

2.7 Cryptographic Key Management

2.7.1 Random Number Generators

The module contains an SP 800-90A approved Hash DRBG. Checks are made to ensure that the quality of the entropy remains high enough to be used to seed the DRBG.

Entropy is provided by a CPU time jitter based non-physical true random number generator. The entropy seeds the DRBG via the /dev/random library.

2.7.2 Key Generation

The module generates keys using an approved key generation mechanism made up of an SP 800-90A Hash DRBG and available entropy conditioned by /dev/random supplemented by the standard Linux Kernel RNG built-in noise source (timing events from storage I/O, inter-process calls (IPCs) and human interface devices (if present)). The module uses 440-bits of entropy to generate keys. Symmetric keys generated by the module are unmodified output from the SP 800-90A DRBG. The key generation provides a security strength of 256-bits.

2.7.3 Key Table

The following tables list all of the keys and CSPs within the module, describe their purpose, and describe how each key is generated, entered and output, stored and destroyed.

Note: "Service" keys. A number of the service APIs are for functions that perform cryptographic operations. Some of these accept keys as parameters. There are also APIs for functions that generate keys and pass them back to the calling application. These keys are ephemeral. They are not stored within the module. After these keys have been used by the API functions, they are zeroized within the module. It is the responsibility of the calling application to ensure that it stores, handles and destroys keys appropriately.

KEY	USE	GENERATION/ESTABLISHMENT	INPUT/OUTPUT	STORAGE	DESTRUCTION
Asymmetric Private Key RSA (2048 or 3072-bits) or ECDSA (P-256, P-384, or P-521 curve).	RSA or ECDSA key pair used for authentication (TLS or IKE).	Internally generated by SP 800-90A DRBG.	N/A	Stored on disk in plaintext.	Zeroized by reformatting the module's hard drive containing the module's firmware.
Asymmetric Public Key RSA (1024[6], 2048 or 3072-bits) or ECDSA (P-256, P-384, or P-521 curve).	RSA or ECDSA key pair used for authentication (TLS or IKE).	Internally generated by SP 800-90A DRBG.	The module's public key is output and the peer's public key is input. Both occur in plaintext.	Stored on disk in plaintext.	Zeroized by reformatting the module's hard drive containing the module's firmware.
Elliptic Curve Diffie-Hellman Private Key	Key exchange during TLS or IKE.	Generated by SP 800-90A DRBG.	N/A	Stored ephemerally in plaintext in RAM.	Zeroized when the session is terminated or power is removed from the module.

[6] 1024-bit RSA only used for signature verification in approved mode of operation

KEY	USE	GENERATION/ESTABLISHMENT	INPUT/OUTPUT	STORAGE	DESTRUCTION
(P-256, P-384, or P-521 curve).					
Elliptic Curve Diffie-Hellman Public Key (P-256, P-384, or P-521 curve).	Key exchange during TLS or IKE.	Generated by SP 800-90A DRBG and established by TLS or IKE negotiations as appropriate.	The module's public key is output and the peer's public key is input. Both occur in plaintext.	Stored on disk in plaintext.	Zeroized when the session is terminated or power is removed from the module.
IPsec Pre-Shared Key (key length is defined by operator).	Authentication of IKE peers	Externally generated.	Key transport via TLS, secured using Session Encryption Keys.	Stored on disk in plaintext.	Zeroized by reformatting the module's hard drive containing the module's firmware.
Session Encryption Keys AES (128 bits, 256 bits).	To secure IPsec and TLS traffic (SIC).	IPsec: Derived via the IKE KDF. TLS: Derived via the TLS KDF.	N/A	Not persistently stored. Cached to disk (plaintext).	Zeroized when the session is terminated or power is removed from the module.
Session HMAC Keys (160 bits, 256 bits, 384 bits or 512 bits depending on size of hash used).	Authenticated TLS traffic (SIC).	Derived via the TLS KDF.	N/A	Cached to disk (plaintext).	Zeroized by reformatting the module's hard drive containing the module's firmware.
Integrity Check key ECDSA P-521 curve certificate.	Module firmware integrity check (ECDSA P-521 key).	Generated outside the module and hardcoded into module firmware.	N/A	Hardcoded into the CPHASH binary in plaintext.	Zeroized by reformatting the module's hard drive containing the module's firmware.
SP 800-90A Hash_DRBG V & C values (440-bits each)	Internal state for the Hash_DRBG random bit generator.	Internal state derived from seed value	N/A	RAM only.	Zeroized when the session is terminated or power is removed from the module.
DRBG Entropy seed **(440 bits)**	Seeds the SP 800-90A DRBG	NDRNG	N/A	RAM only	Zeroized when the session is terminated or power is removed from the module.

Figure 13 Key Table

2.7.4 Access to Key Material

The following table shows the access that an operator has to specific keys or other critical security parameters when performing each of the services relevant to his/her role.

KEY Services SERVICE	Role	Asymmetric Key Pair	Elliptic CurveDiffie-Hellman Key Pairs	IPsec Pre-Shared Key	Session Encryption Keys	Session HMAC Keys	Integrity Check Key	SP 800-90A Hash_DRBG V, C and SeedValues
Symmetric Data Encryption and Decryption for IKE/IPsec	User				U			
Symmetric Data Encryption and Decryption for SIC	User				U			
Message Digest	User							
Keyed Hash	User					U		
Digital Signature Generation	User	U						
Digital Signature Verification	User	U						
RSA Key Generation	CO	W						U
ECDSA Key Generation	CO	W						U
Symmetric Key Generation	CO		W	U	W			U
Show Status	User							
Self-tests	User						U	

Figure 14 Access to keys by services

Access Rights		Blank N/A
	R	Read
	W	Write
	U	Use

2.8 Self-Tests

The module implements both power-up and conditional self-tests as required by FIPS 140-2.

The following two sections outline the tests that are performed.

2.8.1 Power-up self-tests

After power-cycling or booting the appliance the module executes the Power-Up Self-Tests with no further inputs or actions by the operator.

The module implements the following power-up self-tests. The module inhibits all data output while it is operating in the Self-Test state.

OBJECT	TEST
SHA-1	Known answer test
SHA-256	Known answer test
SHA-384	Known answer test
SHA-512	Known answer test
AES-128-CBC Encrypt	Known answer test
AES-128-CBC Decrypt	Known answer test
AES-256-CBC Encrypt	Known answer test
AES-256-CBC Decrypt	Known answer test
AES-128-GCM Encrypt	Known answer test
AES-128-GCM Decrypt	Known answer test
HMAC-SHA-1	Known answer test
HMAC-SHA-256	Known answer test
HMAC-SHA-384	Known answer test
HMAC-SHA-512	Known answer test
Hash DRBG	Known answer test SP 800-90A Section 11.3 Health Tests (instantiate, reseed and generate)
RSA Signature Generation	Known answer test
RSA Signature Verification	Known answer test
ECDSA Signature Generation	Known answer test
ECDSA Signature Verification	Known answer test
KAS-ECC-SSC	Primitive Z computation Known answer test
Firmware Integrity Check	ECDSA P-521 integrity check with SHA-512
IKEv1 KDF	Known answer test
IKEv2 KDF	Known answer test
TLS v1.0/v1.1 KDF	Known answer test
TLSv1.2 KDF	Known answer test

Figure 15 Power-up self-tests

If any of the power-up KATs fail, the system enters an error state. Any self-test errors are output directly to the console output and specific errors are stored in the $FWDIR/log/filesign.elg file. “dmesg” can be run to indicate the status of self-tests.

While in the error state the module inhibits all data output and all cryptographic operations are prohibited. The operator may power cycle the module to re-run the power up self-tests.

2.8.2 Conditional self-tests

The module implements the following conditional self-tests:

EVENT	TEST
Module requests a random number from the FIPS Approved SP800-90A DRBG	A continuous random number generator test
Module requests a random number from the NDRNG used to seed the FIPS Approved SP800-90A DRBG	A continuous random number generator test
Module requests a random number from the FIPS Approved SP800-90A DRBG	SP800-90A Section 11.3 DRBG health tests
RSA key pair is generated	RSA pair-wise consistency test
ECDSA key pair is generated	ECDSA pair-wise consistency test

Figure 16 Conditional self-tests

If any of the conditional self-tests fail, the module shuts down with an error. Any self-test errors are output directly to the console output and specific errors are stored in the $FWDIR/log/filesign.elg file. “dmesg” can be run to indicate the status of self-tests.

While in the error state the module inhibits all data output and all cryptographic operations are prohibited. The operator may power cycle the module to restart the module.

2.9 Design Assurance

Check Point employs industry standard best practices in the design, development, production and maintenance of all of its products, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator's Role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

Delivery of the Cryptographic Module to customers from the vendor is via secure download. The module firmware downloaded can be verified using SHA-256 hash values that are downloaded separately.

2.10 Mitigation of Other Attacks

The module does not mitigate any other attacks.

3 Secure Operation

3.1 Installation

This module firmware can be downloaded from the Check Point Secure Knowledge system.

Once installed, the “cpcrypto ver” command can be used to determine the specific version of the module.

The validated module was tested separately on the Check Point 1530/1535, 1550/1555 and 1570R/1575R Appliances, Check Point 1570/1575 and 1590/1595 Appliances, the Check Point 1600/1800 Appliance, the Check Point 3600 appliance, the Check Point 7000 appliance, the Check Point 16200 Plus appliance, the Check Point 28000 appliance and the HPE DL360 gen 10 hardware.

The module is delivered via the combination of the Main Train (Enterprise appliance and ESX), Scalable Platform (SP), 1530/1535/1550/1555/1570/1570R/1575/1575R/1590/1595 Appliances and 1600/1800 Appliances in the following installation packages:

Item	Download link	Comments
1	Check_Point_R80_30_JUMBO_HF_Bundle_T155_sk153152_Security_ Gateway_3_10_FULL.tgz	Installs on top of the General Availability Release (GA)
2	Check_Point_R80.30_GAIA_3.10_JHF_T155_Hotfix_FIPS_FULL.tgz	Hotfix for R80.30 General Release
3	Check_Point_R80.30_JHF_SP_Hotfix_FIPS_FULL.tgz	Hotfix to R80.30 Saleable Platform (SP) General Release
4	CPinfo	CPinfo build supports Check Point R80 up to R81.20 versions on Gaia OS
5	R81.10 Jumbo Hotfix Accumulator	Jumbo Hotfix for R81.10 Take 75
6	1530/1535/1550/1555/1570/1570R/1575/1575R/1590/1595 Appliances R81.10.05 build 254	Follow the table in the SK for the direct link to the required image
7	1600/1800 Appliances R81.10.05 build 254	Follow the table in the SK for the direct link to the required image

Figure 17 Installation packages

3.1.1 Enterprise appliance and ESX

For the Main Train (Enterprise appliance and ESX) the administrator needs to install:

1. The General Release for R80.30
2. The Jumbo_HF_Bundle_T155_sk152152_Gateway_3_19_FULL (item 1)
3. The Hotfix_FIPS (item 2)
4. CPinfo…. (item 4)

For R81.10, the administrator installs the general release and the Jumbo Hotfix (Item 5) and CPinfo (item 4). Additional actions are not required.

Once installed, the module must be configured to operate in FIPS mode.

This is achieved as follows:

Run “**expert**” and enter desired password:

From the CLI type **set expert-password** then press the Enter key and provide the machine configured password and the new password that you have chosen for the appliance.

Now simple type **expert** and provide the newly configured password. This sets the appliance into expert mode and the rest of the required settings can now be made.

Enable CPU Jitter entropy:

```
chkconfig --add jitterentropy_rngd_init
chkconfig --level 2345 jitterentropy_rngd_init on
```

Run the “**fips on**” shell command from a command-line prompt.

To ensure the module is operating in the approved mode, an operator can observe the following approved mode of operation indicator by executing the **ckp_regedit -p "Software/Checkpoint/SIC”** CLI command: **FIPS_140=[n]1**

3.1.2 Scalable Platform

R81.10 For the Scalable Platform (SP) the administrator needs to install

1. The Scalable Platform General Release
2. The SP_HOTFIX_FIPS_FULL (item 3)
3. CPinfo…. (item 4)

Once installed, the module must be configured to operate in FIPS mode.

This is achieved as follows:

Run “**expert**” and enter desired password:

From the CLI type **set expert-password** then press the Enter key and provide the machine configured password and the new password that you have chosen for the appliance.

Now simple type **expert** and provide the newly configured password. This sets the appliance into expert mode and the rest of the required settings can now be made.

Enable CPU Jitter entropy:

```
chkconfig --add jitterentropy_rngd_init
chkconfig --level 2345 jitterentropy_rngd_init on
```

Run the “**fips on**” shell command from a command-line prompt.

To ensure the module is operating in the approved mode, an operator can observe the following approved mode of operation indicator by executing the **ckp_regedit -p "Software/Checkpoint/SIC”** CLI command: **FIPS_140=[n]1**

3.1.3 1530/1535/1550/1555/1570/1570R/1575/1575R/1590/1595 Appliances and 1600/1800 Appliances

For the 1530/1535/1550/1555/1570/1570R/1575/1575R/1590/1595 Appliances the administrator needs to download item 6 and for the 1600/1800 appliances the administrator needs to download item 7.

Copy the image file to a USB device, connect the USB device to the appliance and reboot it.

Run the “fips on” shell command from a command-line prompt.

To ensure the module is operating in the approved mode, an operator can observe the following approved mode of operation indicator by executing the “fips show” CLI command. This will give the “*FIPS mode is on*“ response text via the CLI.

3.2 Non-approved mode of operation

If the module is not installed according to the instructions in Section 3 the module will be operating non-compliantly. Installing the module as instructed in Section 3 ensures that there aren’t any non-compliant algorithms in the module.

After the module has been installed according to the instructions provided in Section 3 of this Security Policy, there are a number of non-approved algorithms that are not allowed for use in the approved mode that are available to the operator.

SHA-1, when used for signature generation is not allowed. Using SHA-1 for signature generation results in a non-approved mode of operation.

If the operator uses the SHA-1 algorithm with the “Digital Signature Generation” service specified in Figure 12 the module will be operating in the non-approved mode of operation.

Similarly, if an operator accesses a service that uses Triple-DES or Diffie-Hellman variants that are not variants that are not SP 800-56A rev3 compliant, then the module will be operating in a non-approved mode of operation.

3.3 Zeroization

All keys can be zeroized. Ephemeral keys are zeroized by session termination/power cycle. Persistently stored keys can be zeroized by reformatting the hard drive which is not a callable service that the module offers. The module should be under the direct control of the CO when zeroization occurs.