F5, Inc.

F5® vCMP Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Module Version: **15.1.2.1 EHF**

FIPS Security Level 2

document version 1.2

Document Revision: October 2022

Prepared by:
atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Table of Contents

1. Introduction 5
1.1. Cryptographic Module Specification 5
1.1.1. Module Description 5
1.2. FIPS 140-2 Validation Level 5
1.3. Description of modes of operation 6
1.4. Cryptographic Module Boundary 9
1.4.1. Hardware Block Diagram 9
1.4.2. Logical Block Diagram 10
2. Cryptographic Module Ports and Interfaces 11
3. Roles, Services and Authentication 13
3.1. Roles 13
3.2. Authentication 14
3.3. Services 15
4. Physical Security 20
4.1. Tamper Label Placement 20
5. Operational Environment 23
6. Cryptographic Key Management 24
6.1. Key Generation 24
6.2. Key Establishment 24
6.3. Key Entry / Output 25
6.4. Key / CSP Storage 25
6.5. Key / CSP Zeroization 25
6.6. Random Number Generation 25
7. Self-Tests 27
7.1. Power-Up Tests 27
7.1.1. Integrity Tests 27
7.1.2. Cryptographic algorithm tests 27
7.2. ENT (NP) start-up health tests 28
7.3. On-Demand self-tests 28
7.4. Conditional Tests 28
8. Guidance 30
8.1. Delivery and Operation 30
8.2. Crypto Officer Guidance 30
8.2.1. Installing Tamper Evident Labels 30
8.2.2. Initial Configuration 30
8.2.3. Configure vCMP Guest 31
8.2.4. Password Strength Requirement 31
8.2.5. Additional Guidance 31
8.2.6. Version Configuration 32
8.3. User Guidance 32

9. Mitigation of Other Attacks 34

Figure 1-Hardware Block Diagram 10
Figure 2–Logical Block Diagram 10
Figure 3–BIG-IP i5800 and BIG-IP i5820-DF 11
Figure 4–BIG-IP i7800 and BIG-IP i7820-DF 11
Figure 5–BIG-IP i15800 12
Figure 6–VIPRION B2250 12
Figure 7–VIPRION B4450 12
Figure 8–VIPRION B2250 in chassis (1 of 6 tamper labels shown) 20
Figure 9–VIPRION B2250 top view, two sides (5 of 6 tamper labels shown) 21
Figure 10–BIG-IP i5800 and BIG-IP i5820-DF (3 of 3 tamper labels) 21
Figure 11-BIG-IP i7800 and BIG-IP i7820-DF (4 of 4 tamper labels shown) 21
Figure 12-BIG-IP i15800 (Front tamper labels 1-3 labels shown) 22
Figure 13–BIG-IP i15800 (Back tamper labels 4 and 5 labels shown 22
Figure 14–VIPRION B4450 in chassis 22
Figure 15–VIPRION B4450 front (1 of 5 tamper labels shown 22
Figure 16–VIPRION B4450 top-view (4 of 5 tamper labels shown 22

Table 1–Tested Platforms 5
Table 2–Security Levels 6
Table 3 – FIPS Approved Algorithms 8
Table 3a– FIPS non-Approved but Allowed Algorithms in FIPS mode 8
Table 4–Non-FIPS Approved Algorithms/Modes 9
Table 5–Ports and Interfaces 11
Table 6–FIPS 140-2 Roles 14
Table 7–Authentication of Roles 15
Table 8–Management Services in FIPS mode of operation 17
Table 9–Crypto Services in FIPS mode of operation 18
Table 10–Services in non-FIPS mode of operation 19
Table 10a–Non-Authenticated Services 19
Table 11–Inspection of Tamper Evident Labels 20
Table 11a–Number of Tamper Labels per hardware appliance 20
Table 12–Life cycle of CSPs 24
Table 13–Self-Tests 28
Table 14–Conditional Tests 29

Copyrights and Trademarks

F5®, TMOS®, and BIG-IP® are registered trademarks of F5, Inc.

Intel® and Xeon® are registered trademarks of Intel® Corporation.

1. Introduction

This document is the non-proprietary FIPS 140-2 Security Policy of F5® vCMP Cryptographic Module with the firmware version 15.1.2.1 EHF. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 2 module.

1.1. Cryptographic Module Specification

The following section describes the cryptographic module and how it conforms to the FIPS 140-2 specification in each of the required areas.

1.1.1. Module Description

The F5® vCMP Cryptographic Module (hereafter referred to as “the module”) is a firmware module which is a purpose-built hypervisor built on top of F5’s market leading Application Delivery Controller (ADC) technology, and specifically designed for F5 hardware, which allows the segmentation of purpose-built, scalable resources into independent, virtual ADCs.

BIG-IP hardware and software leverages F5’s proprietary operating system, Traffic Management Operating System (TMOS). TMOS is a highly optimized system providing control over the acceleration, security, and management through purpose-built hardware and software systems. The module has been tested on the following multichip standalone devices:

Hardware[1]	Processor	Host OS with hypervisor
VIPRION B2250	Intel® Xeon® E5-2658v2	TMOS 15.1.2.1 EHF with vCMP
VIPRION B4450	Intel® Xeon® E5-2658v3	TMOS 15.1.2.1 EHF with vCMP
BIG-IP i5800	Intel® Xeon® E5-1630v4	TMOS 15.1.2.1 EHF with vCMP
BIG-IP i5820-DF	Intel® Xeon® E5-1630v4	TMOS 15.1.2.1 EHF with vCMP
BIG-IP i7800	Intel® Xeon® E5-1650v4	TMOS 15.1.2.1 EHF with vCMP
BIG-IP i7820-DF	Intel® Xeon® E5-1650v4	TMOS 15.1.2.1 EHF with vCMP
BIG-IP i15800	Intel® Xeon® E5-2680v4	TMOS 15.1.2.1 EHF with vCMP

Table 1–Tested Platforms

1.2. FIPS 140-2 Validation Level

For the purpose of the FIPS 140-2 validation, the F5® vCMP Cryptographic Module is defined as a multi-chip standalone firmware cryptographic module validated at overall security level 2. The table below shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standards.

[1] The module cannot be ported to other operational environment as the IG G.5 only applies at level 1.

FIPS 140-2 Section		Security Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall Level		2

Table 2–Security Levels

1.3. Description of modes of operation

The module must be installed in the FIPS validated configuration as stated in Section 8 – Guidance. In the operation mode, the module supports two modes of operation:

- in "FIPS mode" (the FIPS Approved mode of operation) only approved or allowed security functions with sufficient security strength can be used.
- in "non-FIPS mode" (the non-Approved mode of operation) only non-approved security functions can be used.

The module enters operational mode after power-up tests succeed. Once the module is operational, the mode of operation is implicitly assumed depending on the security function invoked and the security strength of the cryptographic keys. Critical Security Parameters (CSPs) used or stored in FIPS mode are not used in non-FIPS mode, and vice versa.

In the FIPS Approved Mode, the cryptographic module provides the CAVP certificates listed in Table 3. Not all algorithms/modes tested through CAVP are used within the module. Here the Control Plane, or Management, plane refers to the connection from an administrator to the BIG-IP for system management. The Data Plane refers to the traffic passed between external entities and internal servers.

Standards / Algorithm	Usage	Keys / CSPs	Certificate Number	
			Control Plane	Data Plane
[FIPS 197, SP800-38A] AES-ECB, AES-CBC [FIPS 197, SP800-38D] AES-GCM	Encryption and Decryption	128/192/256-bit AES key	A1647	N/A
[FIPS 197, SP800-38A] AES-CBC [FIPS 197, SP800-38D] AES-GCM	Encryption and Decryption	128/ 256-bit AES key	N/A	A1551
[FIPS 197, FIPS 198-1SP800-38F] KTS	Key Wrapping and Unwrapping	128 / 192 / 256-bit AES-CBC key and HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384	A1647	N/A
		128 / 256-bit AES-GCM key	A1647	A1551
		128 / 256-bit AES-CBC key and HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384	A1647	A1551
[SP800-90AReV1] CTR_DRBG AES-256	Random Number Generation with derivation function	Entropy input string seed, V and Key values	A1647	A1551
[FIPS 186-4] RSA	RSA Key Generation	RSA key pair with 2048/3072-bit modulus size	A1647	N/A
RSA PKCS#1 v1.5	RSA Signature Generation and Verification	RSA key pair with 2048/3072-bit modulus with SHA-1(for Sign Ver only), SHA-256 and SHA-384	A1647	A1551
[FIPS 186-4] ECDSA (Appendix B.4.2)	ECDSA Key Pair Generation and Verification (PKV)	ECDSA/ECDH key pair for P-256 and P-384 curves	A1647	A1551
[FIPS 186-4] ECDSA	ECDSA Signature Generation and Verification	ECDSA key pair (P-256 P-384 curves) with SHA-1 (for Sign Ver only), SHA-256 and SHA-384		A1551
[FIPS180-4] SHA-1 SHA-256 SHA-384	Message Digest	N/A	A1647	A1551
[FIPS 198-1] HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	Message Authentication	HMAC key (>=112-bit of strength)	A1647	A1551
KAS-ECC-SSC SP800-56Ar3 Ephemeral Unified	Shared Secret Computation used in Key Agreement Scheme (KAS) IG D.8 scenario X1 (path 2)	Domain Parameter Generation Methods: P-256, and P-384 Ephemeral Unified: KAS Role: initiator, responder	A1647	A1551

Standards / Algorithm	Usage	Keys / CSPs	Certificate Number	
			Control Plane	Data Plane
[SP800-90B] entropy source	Seeding DRBG	Entropy input	ENT (NP)	
[SP800-135] TLS[2] v1.0/1.1 TLS v1.2 with SHA-256 and SHA-384	Key Derivation	TLS pre-primary secret and primary secret and Derived TLS session key (AES, HMAC)	A1647 (CVL)	A1551 (CVL)
[SP800-135] SSH	Key Derivation	SSH Shared Secret and Derived SSH session key (AES, HMAC)	A1647 (CVL)	N/A

Table 3–FIPS Approved Algorithms

Algorithm	Usage	Keys/CSPs
RSA PKCS	Key Wrapping	RSA key pair of 2048 or 3072-bit size
MD5	As part of the TLS v1.0/1.1 key establishment scheme. Allowed in Approved mode with no security claimed per IG 1.23	Digest Size: 128-bit

Table 3a-FIPS non-Approved but Allowed Algorithms in FIPS mode

The Table 4 lists the non-FIPS Approved algorithms along with their usage:

Algorithm	Usage	Notes
AES	Symmetric Encryption and Decryption	using OFB, CFB, CTR, XTS[3] and KW modes, AES-GCM for SSH protocol
DES RC4 Triple-DES SM2, SM4		N/A
CTR_DRBG	Random Number Generation	Underlined algorithm AES-256 cypher, without derivation function
RSA	Asymmetric Encryption and Decryption	using modulus sizes less than 2048-bits or greater than 3072-bits
RSA	Asymmetric Key Generation	FIPS 186-4 less than 2048-bit modulus size
DSA		using any key size
ECDSA		using public/private key pair for curves other than P-256 and P-384

[2] No parts of the TLS protocol except the KDF have been reviewed or tested by the CAVP and CMVP

[3] The AES-XTS mode shall only be used for the cryptographic protection of data on storage devices. The AES-XTS shall not be used for other purposes, such as the encryption of data in transit.

ECDH		
RSA	Digital Signature Generation and Verification	PKCS#1 v1.5 using key sizes other than 2048 and 3072 bits
		PKCS#1 v1.5 using 2048, 3072 bits modulus sIgnature generation: SHA-1, SHA-224, SHA-512 sIgnature verification: SHA-224 and SHA-512
		using X9.31 standard
		using Probabilistic Signature Scheme (PSS)
DSA		using any key size and SHA variant
ECDSA		FIPS 186-4 using curves other than P-256 and P-384
		FIPS 186-4 using curves P-256 and P-384 sIgnature generation: SHA-1, SHA-224, SHA-512 sIgnature verification: SHA-224 and SHA-512
SHA-224 SHA-512 MD5 SM3	Message Digest	N/A
HMAC-SHA-224 HMAC-SHA-512 AES-CMAC Triple-DES-CMAC	Message Authentication	N/A
Diffie-Hellman	Key Agreement Scheme (KAS)	N/A
Ed25519		N/A
ECDH		using curves other than P-256 and P-384
TLS KDF	Key Derivation function	using SHA-224/SHA-512
SSH KDF		using SHA-1/SHA-224/SHA-512
SNMP KDF		using any SHA variant
IKEv1 and IKEv2 KDF		

Table 4–Non-FIPS Approved Algorithms/ Modes

1.4. Cryptographic Module Boundary

The cryptographic boundary of the module is defined by the exterior surface of the appliance (red dotted line in Figure 1). The Figure 1 shows the module, its interfaces and the delimitation of its logical boundary.

1.4.1. Hardware Block Diagram

The block diagram below depicts the major component blocks and the flow of status output (SO), control input (CI), data input (DI) and data output (DO). Description of the ports and interfaces can be found in Table 5.

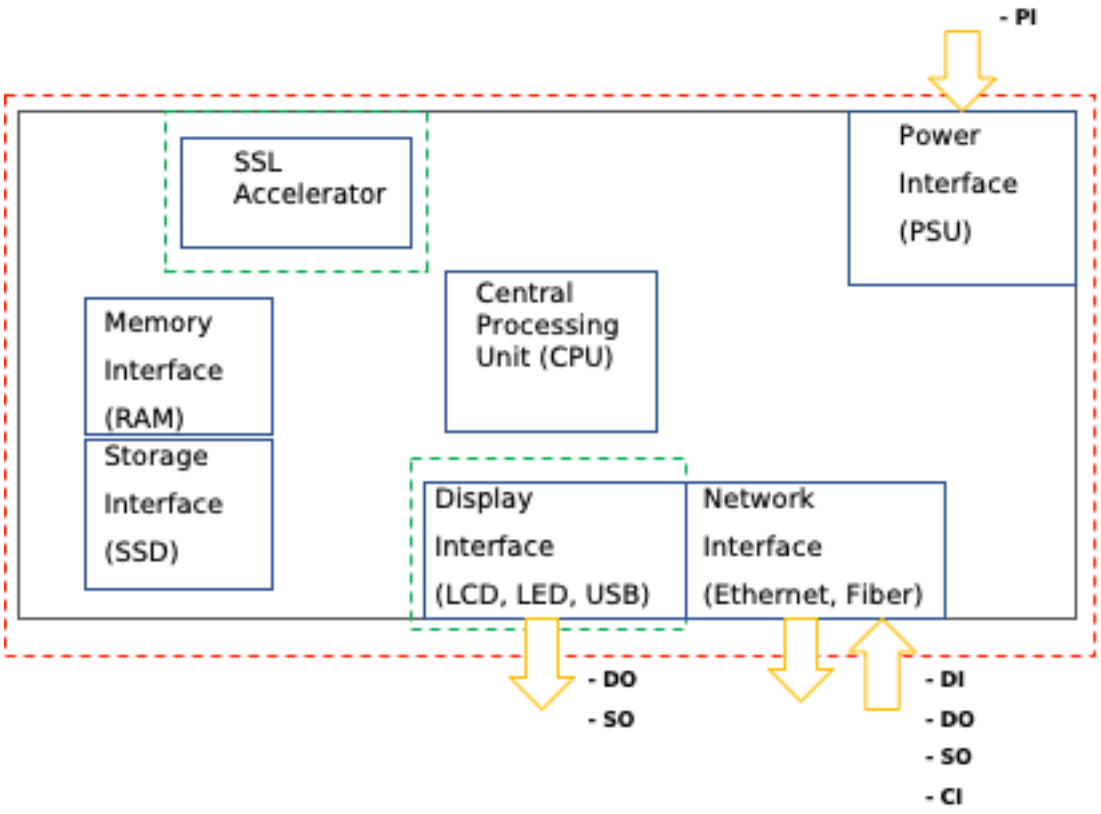

Figure 1-Hardware Block Diagram

1.4.2. Logical Block Diagram

The module's logical boundary consists of the firmware image for the module with the version 15.1.2.1 EHF that runs in the guest environment.

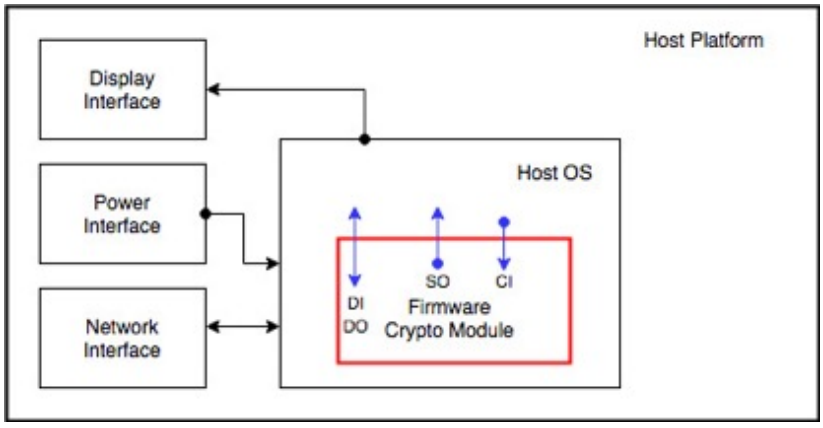

Figure 2–Logical Block Diagram

2. Cryptographic Module Ports and Interfaces

For the purpose of the FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which it runs.

The logical interfaces are the commands through which users of the module request services. The Table 5 summarizes the physical interfaces with details of the FIPS 140-2 logical interfaces they correspond to:

Logical Interface	Physical Interface	Description
Data Input	• Network Interface	Depending on module, the network interface consists of SFP, SFP+, and/or QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 100 Gbps.
Data Output	• Network Interface • Display Interface	Depending on module, the network interface consists of SFP, SFP+, and/or QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 100 Gbps. In addition, status logs may be output to USB found in the interface.
Control Input	• Display Interface • Network Interface	The control input found in the display interface includes the power button and reset button. The control input found in the network interface includes the commands which control module state (e.g. reset module, power-off module). Console port provides capability to remotely power-on, power-off and reset the module. Console access shall not be allowed in operational mode (section 8.2.4)
Status Output	• Display Interface • Network Interface	Depending on module, the display interface can consist of an LCD display, LEDs, and/or output to STDOUT and the USB ports which provide module status information. In addition, command outputs that contain status information flow through the Network Interface. Console port provides capability to remotely read status information. Console access shall not be allowed in operational mode (section 8.2.4)
Power Input	• Power Interface	Power supplies

Table 5–Ports and Interfaces

Figure 3 to Figure 7 depict the various platforms on which the module was tested. Please use the images to familiarize yourself with the devices.

Figure 3–BIG-IP i5800 and BIG-IP i5820-DF

Figure 4–BIG-IP i7800 and BIG-IP i7820-DF

Figure 5–BIG-IP i15800

Figure 6–VIPRION B2250

Figure 7–VIPRION B4450

3. Roles, Services and Authentication

3.1. Roles

The module supports the role-based authentication and the following roles are defined:

- User role: Performs cryptographic services (in both FIPS mode and non-FIPS mode), key zeroization, module status requests, and on-demand self-tests. The FIPS140-2 role of User is mapped to multiple BIG-IP roles which are responsible for different components of the module (e.g. auditing, certificate management, user management, etc.). The User can access the module through Command Line Interface (CLI) or Web Interface described below. However, the CO can restrict User Role access to the CLI. In that case the User will have access through Web Interface only.
- Crypto Officer (CO) role: Crypto officer is represented by the administrator of the BIG-IP. The CO performs module installation and initialization. This role has full access to the module and has the ability to create, delete, and manage other User roles on the module.

The module supports concurrent operators belonging to different roles (one CO and one User role) which creates two different authenticated sessions, achieving the separation between the concurrent operators.

Two interfaces can be used to access the module:

1. CLI: The module offers a CLI called traffic management shell (tmsh) which is accessed remotely using the SSHv2 secured session over the Ethernet ports.
2. Web Interface: The Web interface consists of HTTPS over TLS interface which provides a graphical interface for system management tools. The Web Interface is accessed from a TLS-enabled web browser.

Note: The module does not maintain authenticated sessions upon power cycling. Restarting the module requires the authentication credentials to be re-entered. When entering authentication data through the Web interface, any character entered will be obfuscated (i.e. the character entered is replaced with a dot on the entry box). When entering authentication data through the CLI, the module does not display any character entered by the operator in stdin (e.g. keyboard).

FIPS 140-2 Role	BIG-IP Role	Purpose of Role
Crypto Officer	Administrator	Main administrator of the of the BIG-IP module. This role has complete access to all objects in the module. Entities with this role cannot have other roles within the module.
User	Auditor	Entity who can view all configuration data on the module, including logs
	Certificate Manager	Entity who manages digital certificates and keys.
	Firewall Manager	Grants a user permission to manage all firewall rules and supporting objects. Notably, the Firewall Manager role has no permission to create, update, or delete non-network firewall configurations, including Application Security or Protocol Security policies.
	iRule Manager	Grants a user permission to create, modify, view, and delete iRule. Users with this role cannot affect the way that an iRule is deployed.
	Operator	Grants a user permission to enable or disable nodes and pool members.

FIPS 140-2 Role	BIG-IP Role	Purpose of Role
	Resource Manager	Grants a user access to all objects on the module except BIG-IP user accounts. With respect to user accounts, Resource Manager can view a list of all user accounts on the module but cannot view or change user account properties except for their own user account. User with this role cannot have other user roles on the module.
	User Manager	Entity who manages CO and User Role accounts.

Table 6–FIPS 140-2 Roles

3.2. Authentication

FIPS 140-2 Role	Authentication type and data	Strength of Authentication (Single-Attempt)	Strength of Authentication (Multiple-Attempt)
Crypto Officer	Password based (CLI or Web Interface)	The password must consist of minimum of 6 characters with at least one from each of the three character classes. Character classes are defined as: digits (0-9), ASCII lowercase letters (a-z), ASCII uppercase letters (A-Z). Assuming a worst-case scenario that comprises 6 (six) characters that consist of a set of 4 (four) digits, 1 (one) ASCII lowercase letter and 1 (one) ASCII uppercase letter. The probability to guess every character successfully is (1/10)^4 * (1/26)^1* (1/26)^1 = 1/6,760,000 which is much smaller than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/6,760,000 which is less than the requirement of 1/100,000.
	Signature Verification (CLI only)	The public key used for authentication can either be ECDSA or RSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is:$1/(2^{112})$ which is less than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as $6/(2^{112})$ which is less than the requirement of 1/100,000.
User	Password based (CLI and Web Interface)	The password must consist of minimum of 6 characters with at least one from each of the three character classes. Character classes are defined as: digits (0-9), ASCII lowercase letters (a-z), ASCII uppercase letters (A-Z). Assuming a worst-case scenario that comprises 6 (six) characters that consist of a set of 4 (four) digits, 1 (one) ASCII lowercase letter and 1 (one) ASCII uppercase letter. The probability to guess every character successfully is (1/10)^4 * (1/26)^1 * (1/26)^1 = 1/6,760,000 which is much smaller than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/6,760,000 which is less than the requirement of 1/100,000.

FIPS 140-2 Role	Authentication type and data	Strength of Authentication (Single-Attempt)	Strength of Authentication (Multiple-Attempt)
	Signature Verification (CLI only)	The public key used for authentication can either be ECDSA or RSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is:1/(2^{112}) which is less than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/(2^{112}) which is less than the requirement of 1/100,000.

Table 7–Authentication of Roles

3.3. Services

The module provides services to users that assume one of the available roles. All services are described in detail in the user documentation.

Table 8 lists the services for the management of the module available in FIPS mode of operation which are only available after authentication has succeeded. The Services, the Roles that can request the Service and the CSPs involved and how the CSPs are accessed (Read or Execute / Write / Zeroize -R, W, Z–) are listed.

Service/ Description	Keys/CSPs	Access Type (R, W, Z)	Authorized Role	
			Crypto Officer	User
User Management Services				
List Users Display list of user	N/A	N/A	✓	User Manager Resource Manager Auditor
Create additional users	password	W	✓	User Manager
Modify existing Users	N/A	N/A	✓	User Manager
Delete User	password	Z	✓	User Manager
Unlock User Remove Lock from user who has exceeded login attempts	N/A	N/A	✓	User Manager
Update own password	password	W	All Roles	
Update password for user that is not self	password	W	✓	User Manager
Configure Password Policy Set password policy features	N/A	N/A	✓	N/A
Certificate Management Services				
Create / Delete SSL a self-signed certificate	TLS RSA/ECDSA private Key	W (for Create only)/ R (for Create only) / Z (for Delete only	✓	Certificate Manager Resource Manager

Service/ Description	Keys/CSPs	Access Type (R, W, Z)	Authorized Role	
			Crypto Officer	User
Create / Delete SSL Key used for the SSL Certificate key file	TLS RSA/ECDSA private Key	W (for Create only)/ R (for Create only) / Z (for Delete only	✓	Certificate Manager Resource Manager
List Certificates display or logs expiration date of installed certificates	N/A	N/A	✓	Auditor Certificate Manager Resource Manager
List private keys	N/A	N/A	✓	Auditor Certificate Manager Resource Manager
Import Certificate into module	N/A	N/A	✓	Certificate Manager
Export Certificate File	N/A	N/A	✓	Certificate Manager
ssh-keyswap utility service create or delete ssh keys	Session encryption and authentication keys, ECDH shared secret	R, W, Z	✓	Certificate Manager
Firewall Management Services				
Configure firewall settings set policy rules, and address-lists for use by firewall rules.	N/A	N/A	✓	Firewall Manager
Show firewall state display the current module-wide state of firewall rules	N/A	N/A	✓	Firewall Manager
Show statistics of firewall rules on the BIG-IP system	N/A	N/A	✓	Firewall Manager
Audit Management Services				
View Audit Logs Display logs of configuration	N/A	N/A	✓	Auditor Resource Manager
Export Analytics Logs	N/A	N/A	✓	Auditor
Enable /Disable auditing	N/A	N/A	✓	Resource Manager
System Management Services				
Configure Boot Options Enable Quiet boot, manage boot locations	N/A	N/A	✓	Resource Manager
Configure SSH access options Enable/Disable SSH access, Configure IP address allow list	N/A	N/A	✓	Resource Manager

Service/ Description		Keys/CSPs	Access Type (R, W, Z)	Authorized Role	
				Crypto Officer	User
	Update private key for user authentication	SSH RSA/ECDSA private keys	R,W	✓	User Manager Resource Manager
Configure Firewall Users		N/A	N/A	✓	Firewall Manager
Modify nodes and pool members Enable/Disable nodes and pool members		N/A	N/A	✓	Operator
Configure Node create, modify, view, and delete node					Resource Manager Firewall Manager
Configure iRules create, modify, view, and delete iRules		N/A	N/A	✓	iRule Manager Firewall Manager Resource Manager
Reboot System Restart cryptographic module		N/A	N/A	✓	N/A
Secure Erase Full module zeroization		All CSPs in Table 12	W, Z	✓	N/A

Table 8–Management Services in FIPS mode of operation

Table 9 lists the TLS and SSH crypto services available in FIPS mode of operation and the roles that can request the service, the algorithms and the CSPs involved and how CSPs are accessed (Read/ Write/ Zeroize -R, W, Z-).

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type	Interface	
				R, W, Z	Data Plane	Control Plane
SSH Services						
Establish SSH Session	Signature generation and verification: ECDSA with SHA-256/SHA-384 and curves P-256/P-384 RSA with SHA-256/SHA-384 and 2048/3072-bit key size	User CO	SSH RSA key pair, SSH ECDSA key pair	R		Yes
	Key Exchange: EC Diffie-Hellman		SSH EC Diffie-Hellman key, SSH shared secret	R, W		

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type	Interface	
				R, W, Z	Data Plane	Control Plane
	Key Derivation: SP800-135 SSH KDF		Derived SSH Session encryption key (AES, HMAC) SSH EC Diffie-Hellman shared secret	R, W		
Maintain SSH Session	Data Encryption and Decryption: AES (CBC mode)	User CO	Derived SSH Session encryption key (AES)	R, W		Yes
	Data Integrity (MAC): HMAC with SHA-1		Derived SSH Session data authentication key (HMAC)	R, W		
Close SSH Session	N/A	User CO	All keys and CSPs used in the SSH Establish session and SSH Maintaining session	Z		Yes
TLS Services						
Establish TLS session	Signature Generation and Verification: RSA or ECDSA with SHA-256/ SHA-384	User CO	TLS RSA key pair, TLS ECDSA key pair	R	Yes	Yes
	Key Exchange: ECDH with SP800-135 TLS KDF, RSA Key wrapping (allowed)		TLS RSA key pair, TLS ECDSA key pair, TLS pre-primary secret and primary secret	R, W	Yes	Yes
Maintaining TLS session	Data Encryption: AES CBC, GCM Data Authentication: HMAC SHA-1/ SHA-256/ SHA-384	User CO	Derived TLS session key (AES, HMAC)	R, W	Yes	Yes
Closing TLS session	N/A	User CO	All keys and CSPs used in the TLS Establish session and TLS Maintaining session	Z	Yes	Yes

Table 9–Crypto Services in FIPS mode of operation

Table 10 lists all of the non-approved services available in the non-FIPS-Approved mode of operation.

Service	Role	Usage/Notes
TLS Services		
Establishing TLS session	User / CO	Signature generation and verification using DSA, RSA, ECDSA algorithms listed in Table 4 row *Digital Signature Generation and Verification*
		Key Exchange using: TLS KDF using SHA-224/SHA-512 Diffie-Hellman RSA Key wrapping with keys less than 2048 or greater than 3072-bits ECDH using curves other than P-256 and P-384
Maintain TLS session		Data encryption using Triple-DES, AES-CTR Data authentication using HMAC SHA-224/SHA-512
SSH Services		
Establish SSH session	User / CO	Signature generation and verification using: DSA, RSA, ECDSA algorithms listed in Table 4 row Digital Signature Generation and Verification Key exchange using: SSH KDF using SHA-1/ SHA-224/ SHA-512 Diffie-Hellman, Ed25519, ECDH using curves other than P-256 and P-384
Maintain SSH session		Data encryption using Triple-DES, AES-GCM Data authentication using HMAC SHA-1/SHA-224/SHA-512
Other Services		
IPsec	User / CO	The configuration and usage of IPsec is not approved
iControl REST access		Access to the module through REST using non-approved crypto from Bouncy Castle
Configuration using SNMP		Management of the module via SNMP is not approved.

Table 10–Services in non-FIPS mode of operation

The Table 10a lists the module's services that can be performed without authentication.

Service	Usage/Notes
Show Status	Displays system status information over LCD screen (e.g. network info, system operational status, etc.)
Self-Tests	When the BIG-IP system has been started, the Self-Tests are performed. This includes the integrity check and Known Answer Tests. On-Demand self-tests are initiated by manually power cycling the system.

Table 10a–Non-Authenticated Services

4. Physical Security

All of the platforms listed in Table 1–Tested Platforms are enclosed in a hard-metallic production grade case that provides obscurity and prevents visual inspection of internal components. Each platform is fitted with tamper evident labels to provide physical evidence of attempts to gain access inside the case. The tamper evident labels shall be installed for the module to operate in approved mode of operation. The Crypto Officer is responsible for inspecting the quality of the tamper labels on a regular basis to confirm the modules have not been tampered with. The Crypto Officer must follow instructions provided for proper placement and storage instructions. In the event that additional tamper evident labels are needed, a kit of twenty-five (25) tamper labels is available for purchase (P/N: F5-ADD-BIG-FIPS140). It is the responsibility of the Crypto Officer for the storage of any unused labels.

Physical Security Mechanism	Recommended Inspection Frequency	Guidance
Tamper Evident Labels	Once per month	Check the quality of the tamper evident labels for any sign of removal, replacement, tearing, etc. If any label is found to be damaged or missing, contact the system administrator immediately.

Table 11–Inspection of Tamper Evident Labels

4.1. Tamper Label Placement

The pictures below show the location of all tamper evident labels for each hardware appliance. Label application instructions are provided in the section 8.2.1 below.

Hardware Appliance	# of Tamper Labels	Hardware Appliance	# of Tamper Labels
VIPRION B2250	6	BIG-IP i15800	4
VIPRION B4450	5	BIG-IP i7800	4
BIG-IP i5800	3	BIG-IP i7820-DF	4
BIG-IP i5820-DF	3		

Table 11a–Number of Tamper Labels per hardware appliance

Figure 8–VIPRION B2250 in chassis (1 of 6 tamper labels shown)

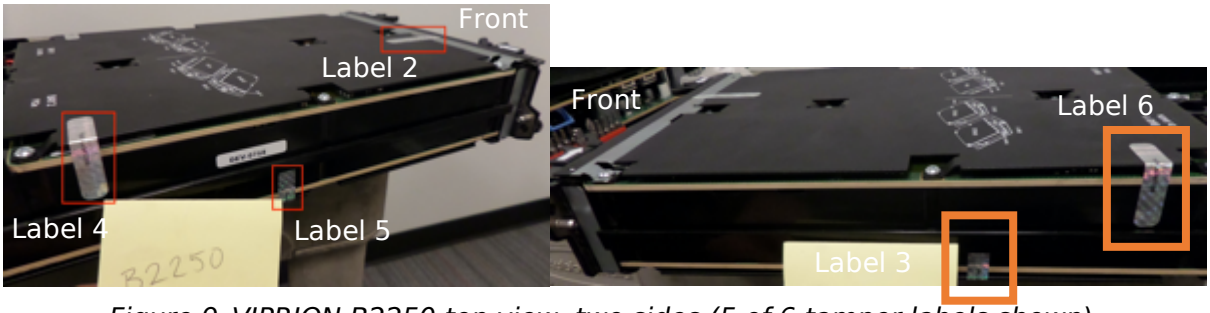

Figure 9–VIPRION B2250 top view, two sides (5 of 6 tamper labels shown)

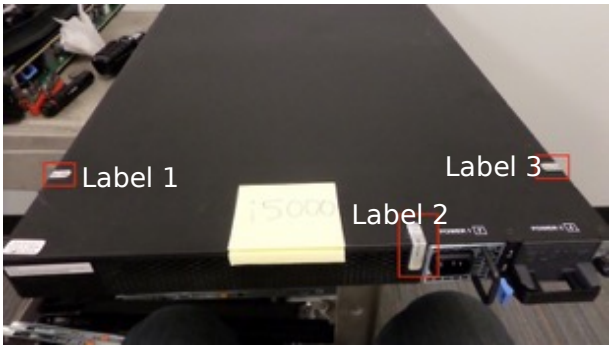

Figure 10–BIG-IP i5800 and BIG-IP i5820-DF (3 of 3 tamper labels)

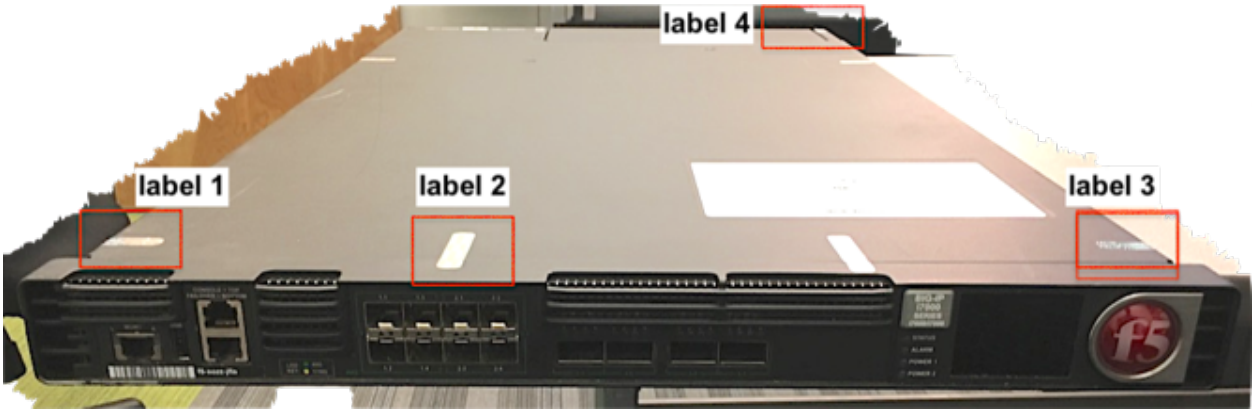

Figure 11-BIG-IP i7800 and BIG-IP i7820-DF (4 of 4 tamper labels shown)

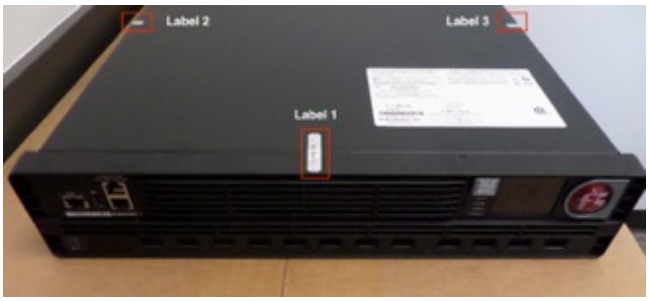

Figure 12-BIG-IP i15800 (Front tamper labels 1-3 labels shown)

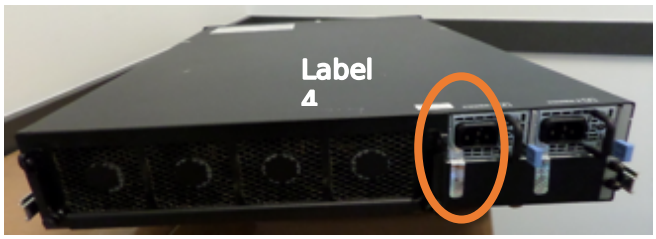

Figure 13–BIG-IP i15800 (Back tamper labels 4 and 5 labels shown

Figure 14–VIPRION B4450 in chassis

Figure 15–VIPRION B4450 front (1 of 5 tamper labels shown

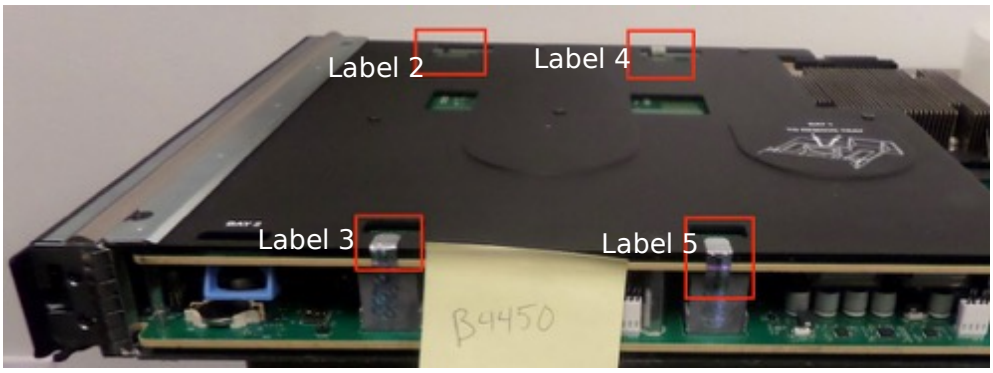

Figure 16–VIPRION B4450 top-view (4 of 5 tamper labels shown

5. Operational Environment

The module operates in a non-modifiable operational environment per FIPS 140-2 level 2 specifications and as such the operational environment requirements do not apply.

6. Cryptographic Key Management

The following table summarizes the CSPs that are used by the cryptographic services implemented in the module. Sizes for the listed keys are given in Table 3 and Table 3a section 1.3.

Name	Generation	Storage	Zeroization
Entropy input string	Obtained from ENT (NP).	RAM	Zeroized by module reboot
DRBG seed, V and Key values	Derived from entropy string as defined by [SP800-90ARev1]	RAM	
TLS RSA signing key pair	Generated using [FIPS 186-4] Key generation method and the random value used in the key generation is generated using [SP800-90ARev1] DRBG.	Disk	Zeroized when key file is deleted or by secure erase option at boot.
TLS ECDSA signing key pair			
TLS RSA wrapping key pair		RAM	Zeroized by closing TLS session or by or rebooting the module.
TLS EC Diffie-Hellman key pair			
TLS Pre-Primary Secret and Primary Secret	Established during the TLS handshake	RAM	Zeroized by closing TLS session or by or rebooting the module.
Derived TLS session key (AES, HMAC)	Derived from the primary secret via [SP800-135] TLS KDF		
SSH Shared Secret	Established during the SSH handshake	RAM	Zeroized by closing SSH session or terminating the SSH application or rebooting the module.
Derived SSH session key (AES, HMAC)	Derived from the shared secret via [SP800-135] SSH KDF	RAM	
SSH EC Diffie-Hellman key pair	Generated using [FIPS 186-4] Key generation method and the random value used in the key generation is generated using [SP800-90ARev1] DRBG.	RAM	
SSH RSA signing key pair		Disk	Zeroized using ssh-keyswap utility or by secure erase option at boot.
SSH ECDSA key pair			
User Password	Entered by the user	Disk	Zeroized by secure erase option at boot or overwritten when password is changed

Table 12–Life cycle of CSPs

6.1. Key Generation

The module implements RSA and EC asymmetric key generation services compliant with [FIPS186-4] and using DRBG compliant with [SP800-90ARev1].

The module does not implement symmetric key generation as an explicit service. The symmetric HMAC and AES keys used by the module are derived from shared secret by applying [SP 800-135] as part of the TLS/SSH protocols. This scenario maps to the section 6.2.1 *Symmetric keys generated using Key agreement scheme* of the [SP 800-133ReV2].

In accordance with [FIPS 140-2 IG] D.12, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per [SP800-133ReV2] (vendor affirmed).

6.2. Key Establishment

The module provides the following key establishment services:

- RSA Key wrapping scheme which is used as part of TLS protocol

- EC Diffie-Hellman key agreement scheme compliant with SP800-56A Rev3 and IG D.8 scenario X1 (path 2) is used as part of the TLS and SSH Protocols. The full ECDH KAS implements a shared secret computation with key derivation implemented by [SP 800-135] TLS and SSH KDFs.
- [SP 800-38F] key wrapping in the context of TLS and SSH protocols where a key may be within a packet or message that is encrypted and authenticated using approved authenticated encryption mode i.e. AES GCM or a combination method which includes approved symmetric encryption algorithm i.e. AES together with approved authentication method i.e. HMAC-SHA.

These schemes provide the following security strength in FIPS mode:

- RSA key wrapping provides 112 or 128-bits of encryption strength
- EC Diffie-Hellman key agreement provides 128 or 192-bits of encryption strength.
- [SP 800-38F] key wrapping using an approved authenticated encryption mode i.e. AES GCM provides 128 or 256 bits of encryption strength (AES-GCM Certs. #A1551 and #A1647) for TLS protocol.
- [SP 800-38F] key wrapping using an approved authenticated encryption mode i.e. AES GCM provides 128 or 256 bits of encryption strength (AES-CBC and HMAC Certs. #A1551 and #A1647) for TLS protocol.
- [SP 800-38F] key wrapping using a combination of approved AES encryption and HMAC authentication method provides between 128 and 256 bits of encryption strength (AES-CBC and HMAC Cert. # A1647) for SSH protocol.

6.3. Key Entry / Output

The module does not support manual key entry or intermediate key generation key output. During the TLS/SSH handshake, the keys that are entered or output to the module over the network, includes RSA/ECDSA public keys and the TLS pre-primary secret encrypted with RSA key only when using the RSA key exchange with TLS. For TLS with ECDH key exchange, the TLS pre-primary secret is established during key agreement and is not output from the module. Once the TLS/SSH session is established, the TLS traffic is protected by AES encryption.

6.4. Key / CSP Storage

As shown in the Table 12 most of the keys are stored in the volatile memory in plaintext form and are destroyed when released by the appropriate zeroization calls or the module is rebooted. The keys stored in plaintext in non-volatile memory are static and will remain on the module across power cycle and are only accessible to the authenticated administrator.

6.5. Key / CSP Zeroization

The zeroization methods listed in the above Table 12, overwrites the memory occupied by keys with “zeros”. Additionally, the user can enforce it by performing procedural zeroization. For keys present in volatile memory, calling reboot command will clear the RAM memory. For keys present in non-volatile memory, using secure erase option (can only be triggered by the administrator during reboot of the module) will perform single pass zero write erasing the disk contents.

6.6. Random Number Generation

The module employs a Deterministic Random Bit Generator (DRBG) based on [SP800-90ARev1] for the generation of random value used in asymmetric keys, and for providing an RNG service to calling applications. The Approved DRBG provided by the module is the CTR_DRBG with AES-256

and derivation function. The DRBG is initialized during module initialization. The module performs DRBG health test according to [SP800-90ARev1] section 11.3.

The module uses a SP800-90B compliant non-physical entropy source ENT (NP) to seed the DRBG. The ENT (NP) provides at least 256-bits of entropy to the DRBG during initialization (seed) and reseeding (reseed). The DRBG is thus capable of supporting a minimum of 256 bits of encryption strength in its output. The ENT (NP) is within its physical boundary.

7. Self-Tests

7.1. Power-Up Tests

The module performs power-up tests automatically during initialization when the module is started without requiring any operator intervention; power-up tests ensure that the module's firmware is not corrupted and that the cryptographic algorithms work as expected.

During the execution of power-up tests, services are not available and input and output are inhibited. Upon successful completion of the power-up tests, the module is initialized and enters operational mode where it is accessible for use. If the module fails any of the power-up tests, except SP 800-90B health tests, then the module enters into the 'Halt Error' state and halts the system. If the module fails any of the SP 800-90B health tests at start-up, then the module enters into the 'Health Test Error' state where it continuously reboots until it is reinstalled. In both error states, the module will prohibit any data outputs and cryptographic operations and will not be available for use. The administrator will need to reinstall the module to continue.

7.1.1. Integrity Tests

The integrity of the module is verified by comparing the MD5 checksum value of the installed binaries calculated at run time with the stored value computed at build time. If the values do not match the module enters 'Halt error' state and the module will not be accessible. In order to recover from this state, the module needs to be reinstalled.

7.1.2. Cryptographic algorithm tests

The module performs self-tests on all FIPS-Approved cryptographic algorithms supported in the approved mode of operation and is done on the Data plane and Control Plane implementations, using the Known Answer Test (KAT) and Pair-wise Consistency Test (PCT) as listed in the following table:

Algorithm	Test
Control Plane Self-tests	
CTR_DRBG	KAT using AES 256-bit with derivation function
AES	KAT of AES encryption and decryption separately with GCM mode and 128-bit key KAT of AES encryption and decryption separately with ECB mode and 128-bit key
RSA	KAT of RSA PKCS#1 v1.5 signature generation with 2048 bit key and SHA-256 KAT of RSA PKCS#1 v1.5 signature verification with 2048 bit key and SHA-256
ECDSA	PCT of ECDSA signature generation and verification with P-256 curve
EC Diffie-Hellman	"Z" computation KAT with P-256 curve
[SP800-135] KDF	SSH KAT TLS v1.0/1.1 and v1.2 KATs
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	KAT of HMAC-SHA-1 KAT of HMAC-SHA-256 KAT of HMAC-SHA-384
SHA-1, SHA-256, SHA-384	Covered by respective HMAC KATs

Algorithm	Test
Data Plane Self-Tests	
AES	KAT of AES encryption and decryption separately with GCM mode and 128-bit key KAT of AES encryption and decryption separately with CBC mode and 128-bit key
RSA	KAT of RSA PKCS#1 v1.5 signature generation with 2048 bit key and SHA-256 KAT of RSA PKCS#1 v1.5 signature verification with 2048 bit key and SHA-256
ECDSA	PCT of ECDSA signature generation and verification with P-256 curve
EC Diffie-Hellman	“Z” computation KAT with P-256 curve
CTR_DRBG	Covered by Control Plane Self-Tests. (Date Plane makes use of the same DRBG implementation provided by Control Plane)
[SP800-135] KDF	TLS v1.0/1.1 and TLS v1.2 KATs
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	KAT of HMAC-SHA-1 KAT of HMAC-SHA-256 KAT of HMAC-SHA-384
SHA-1, SHA-256, SHA-384	Covered by respective HMAC KATs

Table 13–Self-Tests

7.2. ENT (NP) start-up health tests

The SP800-90B health tests (Adaptive Proportion Test -APT- and Repetition Count Test -RCT) are performed at start-up on 1,024 consecutive samples.

7.3. On-Demand self-tests

The module does not explicitly provide the Self-Test service to perform on demand self-tests. On-demand self-tests can be invoked by powering-off and powering-on the module in order to initiate the same cryptographic algorithm tests executed during power-up. During the execution of the on-demand self-tests, crypto services are not available and no data output or input is possible.

7.4. Conditional Tests

The module performs conditional tests on the cryptographic algorithms shown in the following table.

- If the module fails any of the PCTs, the module reboots and enters into the ‘Halt Error’ state.
- If the ENT (NP) health tests fail, then the module moves into the ‘Health Test Error’ state.

In any error states, any data output or cryptographic operations are prohibited. The module will be inoperable. The module must be re-installed in order to clear the error condition.

Algorithm	Test
ENT (NP)	SP800-90B compliant health tests: APT and RCT
RSA key generation	PCT using SHA-256
ECDSA key generation	PCT using SHA-256

Table 14–Conditional Tests

8. Guidance

8.1. Delivery and Operation

The module is distributed as a part of a BIG-IP product which includes the hardware and an installed copy of 15.1.2.1 EHF. The hardware devices are shipped directly from the hardware manufacturer/authorized subcontractor via trusted carrier and tracked by that carrier. The hardware is shipped in a sealed box that includes a packing slip with a list of components inside, and with labels outside printed with the product nomenclature, sales order number, and product serial number. Upon receipt of the hardware, the customer is required to perform the following verifications:

- Ensure that the shipping label exactly identifies the correct customer’s name and address as well as the hardware model.
- Inspect the packaging for tampering or other issues.
- Ensure that the external labels match the expected delivery and the shipped product.
- Ensure that the components in the box match those on the documentation shipped with the product.
- The hardware model can be verified by the model number given on the shipping label as well as on the hardware device itself.

8.2. Crypto Officer Guidance

For FIPS compliance, the following steps must be completed by the Crypto Officer prior to access to the module is allowed.

8.2.1. Installing Tamper Evident Labels

Before the module is installed in the production environment, tamper-evident labels must be installed in the location identified for each module in section 4.1. The following steps shall be taken when installing or replacing the tamper evident labels on the module. The instructions are also included in *F5 Platforms: FIPS Kit Installation* provided with each module.

- Use the provided alcohol wipes to clean the chassis cover and components of dirt, grease, or oil before you apply the tamper evidence seals.
- After applying the seal, run your finger over the seal multiple times using extra high pressure.
- The seals completely cure within 24 hours.

It is the responsibility of the Crypto Officer to inspect the tamper evident labels for damage or any missing labels as specified in Section 4.

8.2.2. Initial Configuration

Follow the instructions in the "BIG-IP System: Initial Configuration" guide to configure the device. The summary of the steps are:

- Run the Setup wizard to license and provision the BIG-IP system.
- Activate the Base Registration Key provided with the purchase of the BIG-IP platform.
- Add the FIPS license. Installing the FIPS license for the host system is required for module activation. Guidance on Licensing the BIG-IP system can be found in https://support.f5.com/csp/article/K7752 and summarized as followed: Before you can activate the license for the BIG-IP system, you must obtain a base registration key. The base registration key is pre-installed on new BIG-IP systems. When you power up the product and connect to the Configuration utility, the licensing page opens and displays the

registration key. After a license activation method is selected (activation method specifies how you want the system to communicate with the F5 License Server), the F5 product generates a dossier which is an encrypted list of key characteristics used to identify the platform. If the automated activation method is selected, the BIG-IP system automatically connects to the F5 License Server and activates the license. If the manual method is selected, the Crypto Officer shall go to the F5 Product Licensing page at secure.f5.com, paste the dossier in the “Enter Your Dossier” box which produces a license. The Crypto Officer will then copy and paste it into the “License” box in the Configuration Utility. The BIG-IP system then reloads the configuration and is ready for additional system configuration. This concludes the product licensing.

8.2.3. Configure vCMP Guest

Each vCMP guest inherits the license of the vCMP host configured above. The license allows you to deploy the maximum number of guests that the platform allows. The crypto officer must follow the “vCMP for Appliance Models: Administration” to create a vCMP guest. A summary is provided below:

1. Provision the vCMP feature as a whole. The BIG-IP system will dedicate most of the disk space to running the vCMP and creates the host portion of the vCMP system.

2. For each guest, the Crypto Officer logs in and provisions the BIG-IP modules. This involves the following:

   Create vCMP guests, including allocating system resources to each guest.

   Create and manage VLANs.

   Manage interfaces

   Configure access control to the host by other host administrators (e.g. User Manager).

3. Set the password requirements and follow additional guidance as documented in Section 8.2.4 below.

Once configured, initialized and POST is completed, the module enters operational state. In this state the mode of operation is implicitly assumed depending on the service invoked. See section 8.3 for details.

8.2.4. Password Strength Requirement

The CO default passwords are marked as expired on the current module at installation. After logging in with the default password, the CO is required to change the password before proceeding. The crypto officer must also modify the BIG-IP password policy to meet or exceed the requirements defined in Table 7–Authentication of Roles. Instructions for this can be found in the “BIG-IP System: User Account Administration” guide. The new passwords must meet the password policy requirements.

8.2.5. Additional Guidance

The Crypto Officer shall verify that the following specific configuration rules are followed in order to operate the module in the FIPS validated configuration:

- All command shells other than tmsh are not allowed. For example, bash and other user-serviceable shells are excluded.
- Management of the module via the appliance's LCD display is not allowed.

- Usage of f5-rest-node and iAppLX and provisioning of iRulesLX is not allowed.
- Only the provisioning of AFM and LTM is included.
- Remote access to the Lights Out / Always On Management capabilities of the module are not allowed.
- Serial port console access from the host platform shall not be allowed after the initial power on and communications setup of the hardware.
- High availability configuration must not be enabled.
- The ‘Single DH use’ option should be turned ON for the platform GUI.
- Use of command *run util fips-util -f init* is not allowed. Running this command followed by a system reboot or restart will mean that the module is not operating as a FIPS validated module.

8.2.6. Version Configuration

Once the module is installed, licensed and configured, the Crypto Officer shall confirm that the module is installed and licensed correctly.

8.2.6.1. Version Confirmation

The Crypto Officer must run the command "tmsh show sys version", then verify that the version shown matches the following:

tmsh show sys version command
Sys::Version
Main Package
Product BIG-IP
Version 15.1.2.1
Edition Engineering Hotfix

Any firmware loaded into the module other than version 15.1.2.1 EHF is out of the scope of this validation and will mean that the module is not operating as a FIPS validated module.

8.2.6.2. License Confirmation

The FIPS validated module activation requires installation of the license referred as ‘FIPS license’.

The Crypto Officer must run the command "tmsh show sys license", then verify that ‘FIPS 140-2’ is in list of Active Modules.

8.3. User Guidance

- The module supports two modes of operation. *Table 9–Crypto Services in FIPS mode of operation* lists the FIPS approved services and *Table 10–Services in non-FIPS mode of operation* lists the non-FIPS approved services. Using the services in *Table 4–Non-FIPS Approved Algorithms/ Modes* means that the module operates in non-FIPS Approved mode for the particular session of a particular service, where the non-FIPS approved algorithm or mode was selected.
- In case the module’s power is lost and then restored, the key used for the AES GCM encryption or decryption shall be re-distributed. The AES GCM IV generation is in compliance with the [RFC5288] and shall only be used for the TLS protocol version 1.2 to be

compliant with [FIPS140-2_IG] IG A.5 scenario 1; thus, the module is compliant with [SP800-52]. The implementation of the nonce_explicit management logic inside the module ensures that when the IV exhausts the maximum number of possible values for a given session key, the module triggers a new handshake request to establish a new key.

9. Mitigation of Other Attacks

The module does not implement security mechanisms to mitigate other attacks.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
ADC	Application Delivery Controller
APT	Adaptive Proportion Test (a SP800-90B continuous health test)
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
CTR	Counter Mode
CVL	Component Validation List
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
KW	Key Wrapping
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
ENT (NP)	Non-Physical Entropy Source
OFB	Output Feedback
PCT	Pair-wise Constancy Test
RCT	Repetition Count Test (a SP800-90B continuous health test)
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
TMOS	Traffic Management Operating System
tmsh	traffic management shell
vCMP	Virtual Clustered Multiprocessing
XTS	XEX-based Tweaked-codebook mode with cipher text stealing

Appendix B. References

FIPS140-2 **FIPS PUB 140-2-Security Requirements For Cryptographic Modules**
May 2001
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS140-2_IG **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**
http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
http://csrc.nist.gov/publications/fips/fips180-4/fips 180-4.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
July 2013
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198 1/FIPS-198 1_final.pdf

PKCS#1 **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography** Specifications Version 2.1 February 2003
http://www.ietf.org/rfc/rfc3447.txt

SP800-38A **NIST Special Publication 800-38A-Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-38D **NIST Special Publication 800-38D-Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
November 2007
http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

SP800-56A Rev3 **NIST Special Publication 800-56A Rev3-Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)**
https://doi.org/10.6028/NIST.SP.800-56Ar3

SP800-90ARev1 **NIST Special Publication 800-90ARev1-Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
June 2015
http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

SP800-131ARev2 **NIST Special Publication 800-131ARev2-Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths**
March 2019
https://doi.org/10.6028/NIST.SP.800-131Ar2