F5® vCMP Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Module Version:

13.1.1 EHF

FIPS Security Level 2

Document Version 1.6

Document Revision: 2019-04-18

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

Copyrights and Trademarks

F5® and BIG-IP® are registered trademarks of F5 Networks.
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 13.1.1 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 optimize 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® E5-2658	TMOS 13.1.1 EHF with vCMP
VIPRION B4450	Intel® Xeon® E5-2658A	TMOS 13.1.1 EHF with vCMP

Table 1 - Tested Platforms

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

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 standard:

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 will provide the following CAVP certified cryptographic algorithms:

Algorithm	Usage	Keys/CSPs	Certificate Number(s)
AES-ECB AES-CBC	Encryption and Decryption	128/192/256-bit AES key	C 50, C 51

AES-GCM			
AES-CBC AES-GCM	Encryption and Decryption	128/256-bit AES key	C 66, C 210
SP800-90A CTR_DRBG	Random Number Generation	Entropy input string, V and Key values	C 50, C 51, C 66, C 210
FIPS 186-4 RSA Key Pair Generation	RSA Key Generation	RSA public and private key pair with 2048/3072-bit modulus size	C 50, C 51
PKCS#1 v1.5 RSA Signature Generation and Signature Verification with SHA-256 and SHA-384	RSA Signature Generation and Verification	RSA private key with 2048/3072-bit modulus	C 50, C 51, C 66, C 210
FIPS 186-4 ECC Key Pair Generation (Appendix B.4.2)	ECDSA Key Pair Generation	ECDSA/ECDH public/private key pair for P-256 and P-384 curves	C 50, C 51, C 66, C 210
FIPS 186-4 ECDSA Signature Generation and Signature Verification	ECDSA Signature Generation and Verification	ECDSA private key (P-256 P- 384 curves)	
SHA-1 SHA-256 SHA-384	Message Digest	N/A	C 50, C 51, C 66, C 210
HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	Message Authentication	HMAC key (>=112-bit)	C 50, C 51, C 66, C 210
SP800-56A ECC except KDF (Section 5.7.1.2 ECC CDH Primitive)	Key Agreement Scheme (KAS) except KDF	private Key with P-256 and P-384 curves	CVL C 50, C 51, C 66, C 210
Key Derivation (KDF used in KAS)	SP800-135 Key Derivation in TLS with SHA-256 and SHA-384	Session encryption and data authentication keys	CVL C 50, C 51, C 66, C 210
	SP800-135 Key Derivation in SSH with SHA-256 and SHA-384		CVL C 50, C 51

Table 3 – FIPS Approved[2]

Algorithm	Usage	Keys/CSPs	Certificate Number(s)
EC Diffie-Hellman	Key Agreement	private Key with P-256 and P-384 curves	Non-Approved but Allowed
RSA PKCS	Key Wrapping	RSA key pair of 2048 or 3072-bit size	Non-Approved but Allowed
NDRNG	DRBG seed generation	seed	Non-Approved but Allowed

Table 3a – FIPS non-Approved but Allowed Algorithms

[2] Please refer to section 6.2 for the strength caveats of the key establishment schemes.

The following table lists the non-FIPS Approved algorithms along with their usage:

Algorithm	Usage	Notes
AES	Symmetric Encryption and Decryption	using OFB, CFB, CTR, XTS and KW modes
DES RC4 Triple-DES		n/a
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 ECDH		using public/private key pair for curves other than P-256 and P-384
RSA	Digital Signature Generation and Verification	PKCS#1 v1.5 using key sizes other than 2048 and 3072 bits
		PKCS#1 v1.5 using SHA-1, 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 with SHA-1, SHA-224 and SHA-512
SHA-224 SHA-512 MD5	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) except KDF	N/A
ECDH		using curves other than P-256 and P-384
TLS KDF	Key Derivation function	using SHA-1/SHA-224/SHA-512
SSH KDF		
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). The block diagram below 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 – Ports and Interfaces* below.

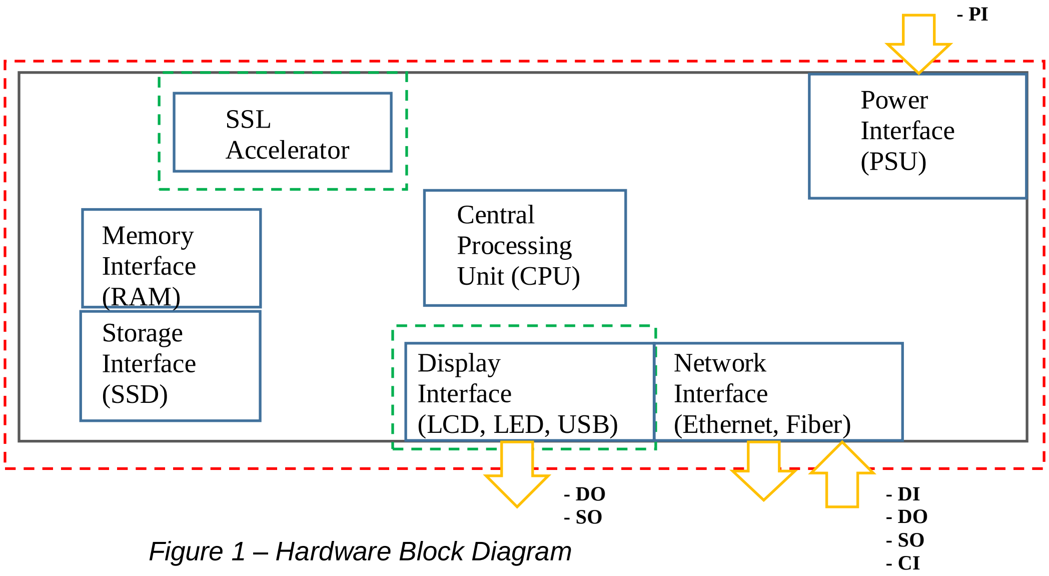

Figure 1 – Hardware Block Diagram

1.4.2. Logical Block Diagram

The module's logical boundary consists of the firmware image for the module with the version 13.1.1 EHF that runs in the guest environment.

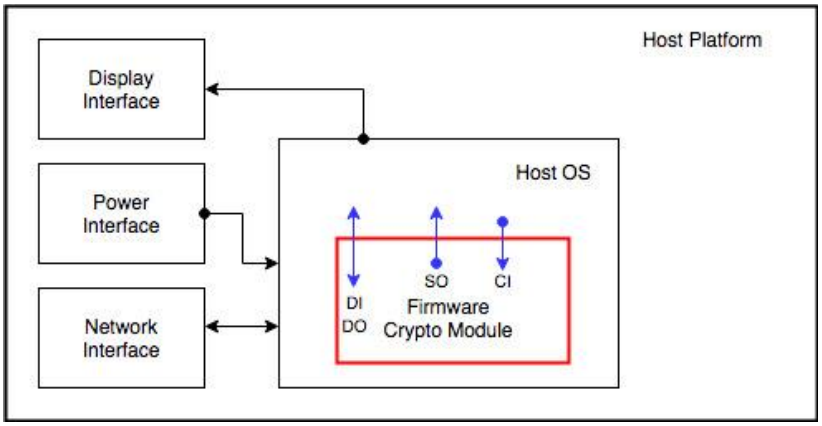

Figure 2 - Logical Block Diagram

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. In Figure 1 above the network interface found on the B2250, consists of one (1) 10/100/1,000 Mbps Ethernet management port, and four (4) 40Gbps QSFP+ ports. On the B4450 the network interface consists of one (1) 10/100/1,000 Mbps Ethernet management port, six (6) 40Gbps QSFP+ ports, two (2) 100Gbps QSFP28 ports and one console port. The display interface found in both the B2250 and B4450 consist of the LEDs and the USB ports. The power interface found in consists of two (B2250) or four (B4450) hot swappable power supplies.

The logical interfaces are the commands through which users of the module request services. The following table summarizes the four 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 One (1) 10/100/1,000 Mbps Ethernet management port, Four (B2250) or Six (B4450) 40Gbps QSFP+ ports, and two (B4450) 100Gbps QSFP28 ports.
Data Output	• Network Interface • Display Interface	Depending on module, the network interface consists One (1) 10/100/1,000 Mbps Ethernet management port, Four (B2250) or Six (B4450) 40Gbps QSFP+ ports, and two (B4450) 100Gbps QSFP28 ports. 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.[3]
Status Output	• Display Interface • Network Interface	Depending on model, the display interface can consist of a LCD display, LEDs, and/or output to STDOUT which provides 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.[3]
Power Input	• Power Interface	Two (B2250) or four (B4450) removable power supplies

Table 5 - Ports and Interfaces

[3] Console access from shall not be allowed in operational mode. Refer to section 8.2.4

The images below show the various test platforms that were tested. Please use the images to familiarize yourself with the devices.

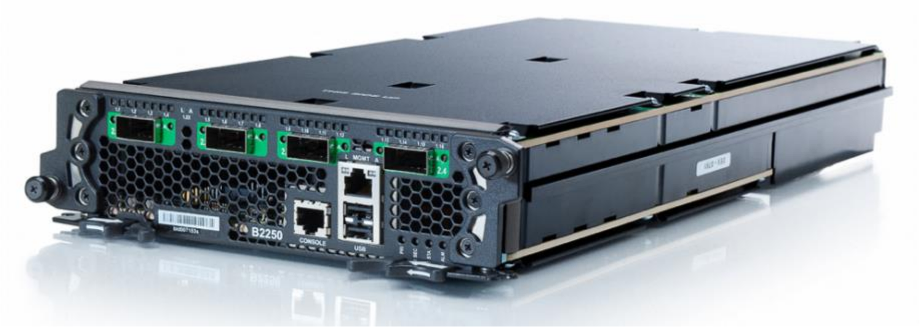

Figure 3 – VIPRION B2250 front panel

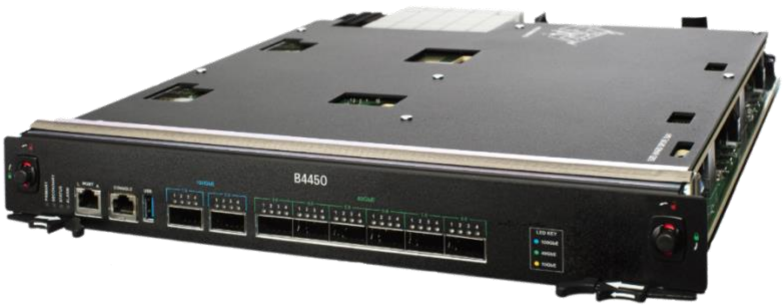

Figure 4 – VIPRION B4450 front panel

3. Roles, Services and Authentication

3.1. Roles

The module supports the role-based authentication and 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 CLI or Web Interface described below. However, the CO can restrict User Role access to the CLI interface. 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. This entity 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.

Two interfaces can be used to access the module:

1. CLI: The module offers a CLI called traffic management shell (tmsh) which can be 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 can be 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. replace the character entered 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 and archives.
	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 iRules. 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. When granted terminal access.

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, a user with this role 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. Users with this role cannot have other user roles on the module.
	User Manager	Entity who manages 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.
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.

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.

The first two tables list the Approved services and the non-Approved but allowed services in FIPS mode of operation and the roles that can request the service. The final table shows the non-FIPS Approved services that only can be executed in the non-FIPS mode along with the corresponding roles.

Table 8 lists the Management Services available in FIPS mode of operation which are only available after authentication has succeeded. Use of any of the following services using non-approve algorithms will place the module in non-approved mode.

Service	Description	Keys/CSPs	Access Type (R[4], W, Z) Read/Write/ Zeroize	Authorization	
				Crypto Officer	User
	User Management Services				
List Users	Display list of user	None	-	✓	User Manager Resource Manager
Create User	Create additional users	password	W	✓	User Manager
View Users	View users	None	-	✓	User Manager
Delete User	Delete users from module	password	Z	✓	User Manager
Unlock User	Remove Lock from user who has exceeded login attempts	None	-	✓	User Manager
Update own password	Update own password	password	W	All Roles	
Update others password	Update password for user that is not self	password	W	✓	User Manager
Configure Password Policy	Set password policy features	None	-	✓	None
	Certificate Management Services				
Create SSL Certificate	Generate a self-signed certificate	RSA/ECDSA private Key	R	✓	Certificate Manager
Create SSL Key	Generate SSL Certificate key file	RSA/ECDSA private Key	W	✓	Certificate Manager
Check-Cert	Examines certificate and display or logs expiration date of installed certificates	None	-	✓	Certificate Manager
List Certificates	Display certificates installed	None	-	✓	Certificate Manager

[4] The R access type refers to Reading of the CSP. This access type can be thought as synonymous to Execute CSP/key.

Service	Description	Keys/CSPs	Access Type (R[4], W, Z) Read/Write/ Zeroize	Authorization	
				Crypto Officer	User
Import SSL Certificate	Import SSL certificate into module	None	-	✓	Certificate Manager
Delete SSL Certificate	Delete a certificate from the module.	None	-	✓	Certificate Manager
Export Certificate File	Export SSL certificate into module	None	-	✓	Certificate Manager
ssh-keyswap utility service	Use ssh-keyswap utility to create or delete ssh keys	Session encryption and authentication keys, EC Diffie-Hellman shared secret	W, Z	✓	Certificate Manager
	Firewall Management Services				
Configure firewall settings	Configure firewall policy rules, and address-lists for use by firewall rules.	None	-	✓	Firewall Manager
Show firewall state	Display the current module-wide state of firewall rules	None	-	✓	Firewall Manager
Show statistics	Displays statistics of firewall rules on the BIG-IP system	None	-	✓	Firewall Manager
	Audit Management Services				
View Audit Logs	Display various service logs	None	-	✓	Auditor
Export Analytics Logs	Export analytics logs	None	-	✓	Auditor
Enable/Disable audition	Enables/Disables auditing	None	-	✓	Auditor
	System Management Services				
Configure Boot Options	Enable Quit boot, manage boot locations	None	-	✓	Resource Manager
Configure SSH access options	Enable/Disable SSH access, Configure IP address whitelist	None	-	✓	None
Configure Firewall Users	Manage firewall rules	None	-	✓	Firewall Manager
Configure nodes and pool members	Enable/Disable nodes and pool members	None	-	✓	Operator
Configure iRules	create, modify, view, and delete iRules	None	-	✓	iRule Manager

Service	Description	Keys/CSPs	Access Type (R[4], W, Z) Read/Write/ Zeroize	Authorization	
				Crypto Officer	User
Self-Test	Restart cryptographic module to perform on-demand self-test	None	-	✓	Resource Manager
Show Status	Show cryptographic module status (i.e version, hardware info, etc.)	None	-	✓	All
Secure Erase	Full module zeroization	All CSPs in Table 12.	W, Z	✓	None

Table 8 –Management Services in FIPS mode of operation

Table 9 lists the crypto services available in FIPS mode of operation. Here the Control Plane refers to connecting to the module for management and the Data Plane refers to the connection of the module to external entities.

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type (R, W, Z) Read/Write/Zeroize	Interface	
SSH Services					**Data Plane**	**Control Plane**
Establish SSH Session	Signature generation and verification: ECDSA with SHA-256/SHA-384 and curve P-256/P-384 RSA with SHA-256/SHA-384 and 2048/3072-bit key size	User CO	RSA/ECDSA signing key	R, W		Yes
	Key Exchange: EC Diffie-Hellman		EC Diffie-Hellman key, shared secret	R, W		
	Key Derivation: SP800-135 SSH KDF		Session encryption keys EC Diffie-Hellman shared secret	R, W		
Maintain SSH Session	Data Encryption and Decryption: AES (CBC mode)	User CO	Session encryption keys	R, W		Yes
	Data Integrity(MAC): HMAC with SHA-1		Session data authentication keys	R, W		
Close SSH Session	N/A	User CO	Zeroize session keys and shared secret	Z		Yes

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type (R, W, Z) Read/Write/Zeroize	Interface	
TLS Services					Data Plane	Control Plane
Establish TLS session	Signature Generation and Verification: RSA or ECDSA with SHA-256/SHA-384	User CO	RSA, ECDSA signing key	R, W	Yes	Yes
	Key Exchange: ECDH with SP800-135 TLS KDF, RSA Key wrapping (allowed)		RSA wrapping key, ECDH Key, TLS pre-master secret and master secret	R, W	Yes	Yes
Maintaining TLS session	Data Encryption: AES CBC, GCM Data Authentication: HMAC SHA-1/SHA-256/SHA-384	User CO	AES and HMAC Keys	R, W	Yes	Yes
Closing TLS session	N/A	User CO	Zeroize session keys, shared secret	Z	Yes	Yes

Table 9 –Crypto Services in FIPS mode of operation

The following tables list 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 or RSA/ECDSA with SHA-1/SHA-224/SHA-512 RSA with keys less than 2048
		Key Exchange using: Diffie-Hellman RSA Key wrapping with keys less than 2048 or greater than 3072
Maintain TLS session		Data encryption using Triple-DES Data authentication using HMAC SHA-224/SHA-512
SSH Services		

Service	Role	Usage/Notes
Establish SSH session	User CO	Signature generation and verification using: DSA, Ed25519 RSA/ECDSA with SHA-1/SHA-224/SHA-512 RSA with key size less than 2048-bit Key exchange using Diffie-Hellman, Ed25519
Maintain SSH session		Data encryption using Triple-DES 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 BouncyCastle
Configuration using SNMP		Management of the module via SNMP is not approved.

Table 10 – Services in non-FIPS mode of operation

4. Physical Security

All of the platforms listed in *Table 1: Tested Platforms* are enclosed in a hard-metallic case that provides obscurity from 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 is available for purchase (P/N: F5-ADD-BIG-FIPS140). The kit comes with twenty-five (25) tamper labels. 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 details below show the location of all tamper evident labels for each platform. Label application instructions are provided in the *F5 Platforms: FIPS Kit Installation* guide delivered with each platform.

Module	Number of Tamper Labels
VIPRION B2250	6
VIPRION B4450	5

Table 121a Number of Tamper Labels per Module

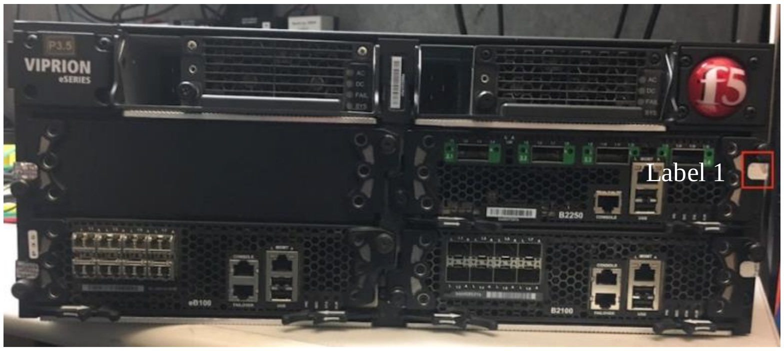

Figure 5 – VIPRION B2250 in chassis (1 of 6 tamper labels shown)

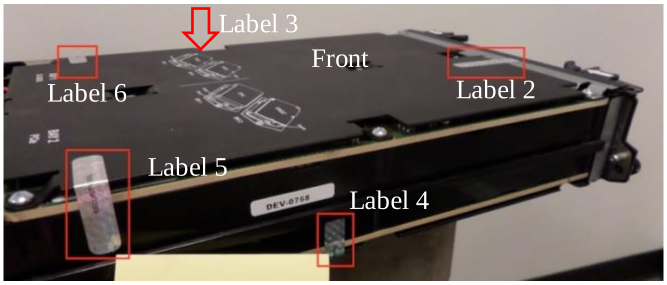

Figure 6 - VIPRION B2250 top view (5 of 6 tamper labels shown)

Figure 7 - VIPRION B4450 in chassis

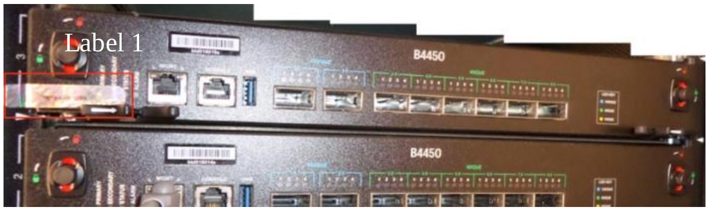

Figure 8 – VIPRION B4450 front (1 of 5 tamper labels shown)

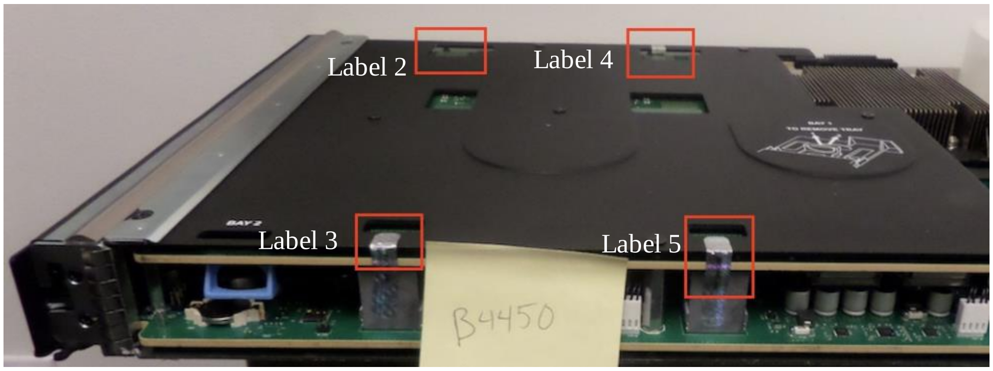

Figure 9 - VIPRION B4450 top-view (4 of 5 tamper labels shown)

5. Operational Environment

5.1. Applicability

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:

Name	Generation	Storage	Zeroization
DRBG entropy input string	Obtained from NDRNG.	RAM	Zeroized by module reboot
DRBG seed, V and Key values	Derived from entropy string as defined by [SP800-90A]	RAM	
TLS RSA signing private key	Generated using FIPS 186-4 Key generation method and the random value used in the key generation is generated using SP800-90A DRBG.	Disk	Zeroized when key file is deleted or by secure erase option at boot.
TLS ECDSA signing private key			
TLS RSA wrapping private key		RAM	Zeroized by closing TLS session or by or rebooting the module.
TLS EC Diffie-Hellman private Key			
TLS Pre-Master Secret and Master 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 master 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 private Key	Generated using FIPS 186-4 Key generation method and the random value used in the key generation is generated using SP800-90A DRBG.	RAM	
SSH RSA signing private Key		Disk	Zeroized using ssh-keyswap utility or by secure erase option at boot.
SSH ECDSA signing private Key			
User Password	Entered by the user	Disk	Zeroized by secure erase option at boot or overwritten when password is changed

Table 13 - Life cycle of CSPs

The following sections describe how CSPs, in particular cryptographic keys, are managed during its life cycle.

6.1. Key Generation

The HMAC and AES keys are generated as part of the TLS/SSH protocol when deriving session keys. For generation of RSA and EC keys, the module implements asymmetric key generation services compliant with [FIPS186-4] and using DRBG compliant with [SP800-90A]. A seed (i.e. the random value) used in asymmetric key generation is obtained from [SP800-90A] DRBG. The module does not implement symmetric key generation as an explicit service. The symmetric keys used are derived from shared secret by applying SP 800-135 as part of the TLS/SSH protocol. This scenario maps to the section 7.3 of the SP 800-133 symmetric keys generated using Key agreement scheme. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per SP800-133 (vendor affirmed).

6.2. Key Establishment

The module provides RSA Key wrapping scheme which is used as part of TLS protocol and EC Diffie-Hellman key agreement scheme which is used as part of the TLS and SSH Protocol with the key derivation implemented by SP 800-135 TLS and SSH KDF. The module also includes a SP 800-38F key wrapping in the context of TLS and SSH protocol 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 between 128 and 256 bits of encryption strength
- SP 800-38F key wrapping using a combination of an approved AES encryption and HMAC authentication method provides between 128 and 256 bits of encryption strength

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-master secret encrypted with RSA key only when using the RSA key exchange with TLS. For TLS with ECDH key exchange, the TLS pre-master 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 above table 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, 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 [SP800-90A] 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. The DRBG is initialized during module initialization. The module performs DRBG health test according to [SP800-90A] section 11.3.

The module uses a Non-Deterministic Random Number Generator (NDRNG) to seed the DRBG. A Continuous Random Number Generation Test (CRNGT) is performed on the output of the NDRNG prior to seeding the DRBG and also on the DRBG output. The NDRNG provides at least 256- bits of entropy to the DRBG during initialization (seed) and reseeding (reseed). The NDRNG 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, it enters into the 'Halt Error' state and halts the module. In this state, the module will prohibit any data outputs and cryptographic operations and will not be available for use. The module will be marked unusable and 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 as well as Control Plane side, 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 and without derivation function
AES	• KAT of AES encryption with ECB mode and 128-bit key • KAT of AES decryption 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	• primitive “Z” computation KAT with P-256 curve
SHA-1, SHA-256, SHA-384	• KAT of SHA-1 • KAT of SHA-256 • KAT of SHA-384 is covered by KAT for HMAC-SHA-384
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	• KAT of HMAC-SHA-1 • KAT of HMAC-SHA-256 • KAT of HMAC-SHA-384

Algorithm	Test
Data Plane Self-Tests	
AES	• KAT of AES encryption with CBC mode and 128-bit key • KAT of AES decryption 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	• primitive “Z” computation KAT with P-256 curve
CTR_DRBG	• Covered by Data Plane Self-Tests. (Control Plane makes use of the same DRBG implementation provided by Data Plane)
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 14- Self-Tests

7.2. 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.

7.3. Conditional Tests

The module performs conditional tests on the cryptographic algorithms shown in the following table. If the module fails any of these tests, the module reboots and enters into the Halt Error state prohibiting any data output or cryptographic operations and the module will be inoperable. The module must be re-installed in order to clear the error condition.

Algorithm	Test
DRBG	• Continuous random number generator test (CRNGT) on the output of the DRBG
NDRNG	• Continuous random number generator test (CRNGT) on the output of the NDRNG prior to seeding the CTR_DRBG
RSA key generation	• Pair-wise Consistency Test (PCT) using SHA-256
ECDSA key generation	• Pair-wise Consistency Test (PCT) using SHA-256

Table 15 - 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 13.1.1 EHF. For FIPS compliance, the following steps defined in section 8.2 must be completed by the Crypto Officer prior to access to the module is allowed.

8.2. Crypto Officer Guidance

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. Install Module

- Follow the instructions in the "*BIG-IP System: Initial Configuration*" guide to configure and install the FIPS license for the host system required for module activation.
- Configure vCMP Guests: The crypto officer must follow the *“vCMP for VIPRION Systems: Administration”* to create a vCMP guest.
- Set the password requirements and follow additional guidance as documented in the steps 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.

8.2.3. Password Strength Requirement

The Crypto officer must create his own password after assuming the role for the first time. The crypto officer must then modify the BIG-IP password policy to meet or exceed the requirements defined in Table 5 – Authentication of Roles. Instructions for this can be found in the “*BIG-IP System: User Account Administration*” guide. For SSH authentication the Crypto officer must configure the SSH to allow only password-based authentication.

8.2.4. 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.

8.2.5. Version Configuration

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

8.2.5.1. Version Confirmation

The Crypto Officer must run the command "tmsh show sys version", then verify the version shown with the approved version from Table 1 - Tested Platforms.

8.2.5.2. 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 the list of license flags includes the "FIPS 140-2 Compliant Mode".

8.3. User Guidance

- The module supports two modes of operation. *Table 9 –Crypto Services in FIPS mode of operation* list 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; thus, the module is compliant with [SP800-52]

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
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
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
NDRNG	Non-Deterministic Random Number Generator
OFB	Output Feedback
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
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
December 2017
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
NIST Special Publication 800-56A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
March 2007
http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf

SP800-90A
NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators
January 2012
http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf

SP800-131A
NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
November 2015
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf