

F5, Inc



F5® Device Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Hardware Versions:

BIG-IP i4600, BIG-IP i4800, BIG-IP i5600, BIG-IP i5800, BIG-IP i5820-DF, BIG-IP i7600, BIG-IP i7800, BIG-IP i7820-DF, BIG-IP i10600, BIG-IP i10800, BIG-IP i11600-DS, BIG-IP i11800-DS, BIG-IP i15600, BIG-IP i15800, BIG-IP 10350v-F, VIPRION B2250 and VIPRION B4450

with FIPS Kit P/N: F5-ADD-BIG-FIPS140

Firmware Version: 15.1.2.1 EHF

FIPS Security Level 2

Document Version 1.3

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	Cryptographic Module Specification.....	6
1.1	Module Description	6
1.2	FIPS 140-2 Validation Level.....	7
1.3	Description of modes of operation	8
1.4	Cryptographic Module Boundary.....	12
2	Cryptographic Module Ports and Interfaces.....	14
3	Roles, Services and Authentication.....	17
3.1	Roles	17
3.2	Authentication.....	19
3.3	Services	20
4	Physical Security	27
4.1	Tamper Label Placement	27
5	Operational Environment	32
6	Cryptographic Key Management.....	33
6.1	Key Generation	33
6.2	Key Establishment	34
6.3	Key Entry / Output	35
6.4	Key / CSP Storage	35
6.5	Key / CSP Zeroization.....	35
6.6	Random Number Generation	35
7	Self-Tests.....	36
7.1	Power-Up Tests	36
7.1.1	<i>Integrity Tests</i>	<i>36</i>
7.1.2	<i>Cryptographic algorithm tests.....</i>	<i>36</i>
7.2	ENT (NP) start-up health tests.....	38
7.3	On-Demand self-tests	38
7.4	Conditional Tests	38
8	Guidance.....	39
8.1	Delivery and Operation	39
8.2	Crypto Officer Guidance.....	39
8.2.1	<i>Installing Tamper Evident Labels.....</i>	<i>39</i>
8.2.2	<i>Install Device.....</i>	<i>40</i>
8.2.3	<i>Password Strength Requirement</i>	<i>40</i>
8.2.4	<i>Additional Guidance</i>	<i>41</i>

8.2.5 Version Configuration 41

8.3 User Guidance.....42

9 Mitigation of Other Attacks43

Figure 1 - Hardware Block Diagram 13

Figure 2 - BIG-IP i4600 and BIG-IP i4800 14

Figure 3 - BIG-IP i5600, BIG-IP i5800 and BIG-IP i5820-DF 14

Figure 4 - BIG-IP i7600, BIG-IP i7800 and BIG-IP i7820-DF 15

Figure 5 - BIG-IP i10600, BIG-IP i10800 and BIG-IP i11600-DS, BIG-IP i11800-DS 15

Figure 6 - BIG-IP i15600, BIG-IP i15800..... 15

Figure 7 - BIG-IP 10350v-F 15

Figure 8 - VIPRION B2250..... 15

Figure 9 - VIPRION B4450..... 16

Figure 10 - Tamper labels on BIG-IP i4600 and BIG-IP i4800..... 28

Figure 11 - Tamper labels on BIG-IP i5600, BIG-IP i5800 and BIG-IP i5820-DF..... 28

Figure 12 - Tamper labels on BIG-IP i7600, BIG-IP i7800 and BIG-IP i7820-DF..... 29

Figure 13 - Tamper labels on BIG-IP i10800, BIG-IP i10600 and BIG-IP i11600-DS, BIG-IP i11800-DS 29

Figure 14 - Tamper labels on BIG-IP i15600, BIG-IP i15800. 30

Figure 15 - Tamper labels on BIG-IP 10350v-F. 30

Figure 16 - Tamper labels on VIPRION B2250 in chassis..... 31

Figure 17 - Tamper labels on top view VIPRION B2250, and two sides VIPRION B2250..... 31

Figure 18 - Tamper labels on VIPRION B4450 top-view..... 31

Figure 19 - Tamper labels on VIPRION B4450 in chassis..... 31

Table 1 - Tested Modules 7

Table 2 - Security Levels..... 8

Table 3 - Approved Cryptographic Algorithms 10

Table 4 - non-Approved but Allowed in FIPS mode Cryptographic Algorithms 11

Table 5 - Non-Approved and Non-Compliant Cryptographic Algorithms/Modes 12

Table 6 - Ports and Interfaces 14

Table 7 - FIPS 140-2 Roles 18

Table 8 - Authentication of Roles..... 20

Table 9 - Non-Authenticated Services..... 20

Table 10 - Authenticated Management Services in FIPS mode of operation..... 23

Table 11 - Crypto Services in FIPS mode of operation 25

Table 12 – Services in non-FIPS mode of operation..... 26

Table 13 – Inspection of Tamper Evident Labels 27

Table 14 – Number of Tamper Evident Labels per hardware appliance 28

Table 15 – Life cycle of CSPs 33

Table 16 – Self-Tests 37

Table 17 – Conditional Tests 38

Copyrights and Trademarks

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

Introduction

This document is the non-proprietary FIPS 140-2 Security Policy of F5® Device Cryptographic Module with firmware version 15.1.2.1 EHF and hardware version listed in Table 1. 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 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 Module Description

The F5® Device Cryptographic Module (hereafter referred to as “the module”) is a smart evolution of Application Delivery Controller (ADC) technology. Solutions built on this platform are load balancers. They are full proxies that give visibility into, and the power to control—inspect and encrypt or decrypt—all the traffic that passes through your network. Underlying all BIG-IP hardware and software is F5’s proprietary operating system, TMOS, which provides unified intelligence, flexibility, and programmability. With its application control plane architecture, TMOS gives you control over the acceleration, security, and availability services your applications require. TMOS establishes a virtual, unified pool of highly scalable, resilient, and reusable services that can dynamically adapt to the changing conditions in data centers and virtual and cloud infrastructures. The module has been tested on the hardware platforms listed in Table 1 with the firmware version 15.1.2.1 EHF.

Hardware	Processor	Operating System	Ports ¹
BIG-IP i4600 BIG-IP i4800	Intel® Xeon® D- 1518	TMOS 15.1.2.1 EHF	1 x USB port 8 x 1GbE; 4 x 10GbE network ports 1 x Console port 1 x 1GbE management port
BIG-IP i5600 BIG-IP i5800 BIG-IP i5820-DF	Intel® Xeon® E5- 1630v4	TMOS 15.1.2.1 EHF	1 x USB port 8 x 10GbE; 4 x 40GbE network ports 1 x Console port 1 x 1GbE management port
BIG-IP i7600 BIG-IP i7800 BIG-IP i7820-DF	Intel® Xeon® E5- 1650v4	TMOS 15.1.2.1 EHF	1 x USB port 8 x 10GbE and 4 x 40GbE network ports 1 x Console port 1 x 10/100/1000-BaseT management port
BIG-IP i10600 BIG-IP i10800	Intel® Xeon® E5- 1660v4	TMOS 15.1.2.1 EHF	1 x USB port 8 x 10GbE; 6 x 40GbE network ports 1 x Console port 1 x 1GbE management port

¹ The USB port found on all platforms are used only for exporting the audit logs

Hardware	Processor	Operating System	Ports ¹
BIG-IP i11600-DS BIG-IP i11800-DS	Intel® Xeon® E5- 2695v4	TMOS 15.1.2.1 EHF	1 x USB port 8 x 10GbE; 6 x 40GbE network ports 1 x Console port 1 x 1GbE(10/100/1000 capable) management port
BIG-IP i15600 BIG-IP i15800	Intel® Xeon® E5- 2680v4	TMOS 15.1.2.1 EHF	1 x USB port 8 x 40GbE; 4 x 100GbE network ports 1 x Console port 1 x 1GbE management port
BIG-IP 10350v-F	Intel® Xeon® E5- 2658v2	TMOS 15.1.2.1 EHF	2 x USB port 16 x 1/10GbE; 2 x 40GbE network ports 1 x Console port 1 x 10/100/1000-BaseT management port
VIPRION B2250	Intel® Xeon® E5- 2658v2	TMOS 15.1.2.1 EHF	2 x USB port 4 x 40 GbE network ports 1 x Console port 1 x GbE management port
VIPRION B4450	Intel® Xeon® E5- 2658v3	TMOS 15.1.2.1 EHF	1 x USB port 6 x 40 GbE; 2 x 100 GbE network ports 1 x Console port 1 x GbE (10/100/1000 Ethernet) management port

Table 1 - Tested Modules

1.2 FIPS 140-2 Validation Level

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

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 self-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 following CAVP certificates (Table 3). The Control (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	A1351	N/A
[FIPS 197, SP800-38A] AES-CBC [FIPS 197, SP800-38D] AES-GCM		128 / 256-bit AES key	N/A	A1350
[FIPS 197, SP800-38F, FIPS 198-1] KTS	Key Wrapping and Unwrapping	128 / 192 / 256-bit AES- CBC key and HMAC-SHA- 1, HMAC-SHA-256, or HMAC-SHA-384	A1351	N/A
		128 / 256-bit AES-GCM key	A1351	A1350
		128 / 256-bit AES-CBC key and HMAC-SHA-1, HMAC- SHA-256, or HMAC-SHA- 384	A1351	A1350
[SP800-90ARev1] CTR_DRBG	Random Number Generation with derivation function	Entropy input string seed, V and Key values	A1351	A1350
[FIPS 186-4] RSA	RSA Key Generation	RSA key pairs with 2048/ 3072-bit modulus size	A1351	N/A
PKCS#1 v1.5 RSA	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	A1351	A1350
[FIPS 186-4] (Appendix B.4.2) ECC Key Pair Generation	ECDSA Key Pair Generation / Verification	ECDSA/ ECDH key pair with P-256 and P-384 curves	A1351	A1350
[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	A1351	A1350

Standards/ Algorithm	Usage	Keys/CSPs	Certificate Number	
			Control Plane	Data Plane
[FIPS180-4] SHA-1 SHA-256 SHA-384	Message Digest	N/A	A1351	A1350
[FIPS 198-1] HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	Message Authentication	HMAC key (>=112-bit)	A1351	A1350
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, P-384 Ephemeral Unified: KAS Role: initiator, responder	A1351	A1350
[SP800-135] SSH	Key Derivation	SSH Shared Secret and Derived SSH session key (AES, HMAC)	A1351 (CVL)	N/A
[SP800-135] TLS ² v1.0/1.1 and TLS v1.2 with HMAC-SHA-256 and HMAC-SHA- 384		TLS pre-primary secret and primary secret and Derived TLS session key (AES, HMAC)	A1351 (CVL)	A1350 (CVL)
[SP800-90B] entropy source	Seeding DRBG	Entropy input	ENT (NP)	

Table 3 - Approved Cryptographic Algorithms

The following table lists the non-Approved algorithms that are allowed in FIPS approved mode along with their usage.

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

Algorithm	Usage	Keys/CSPs
PKCS#1 v1.5 RSA Key Wrapping	Asymmetric Encryption and Decryption	RSA key pair with 2048/3072-bit modulus.
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 4 - non-Approved but Allowed in FIPS mode Cryptographic Algorithms

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 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 or greater than 3072 bits
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 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)

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

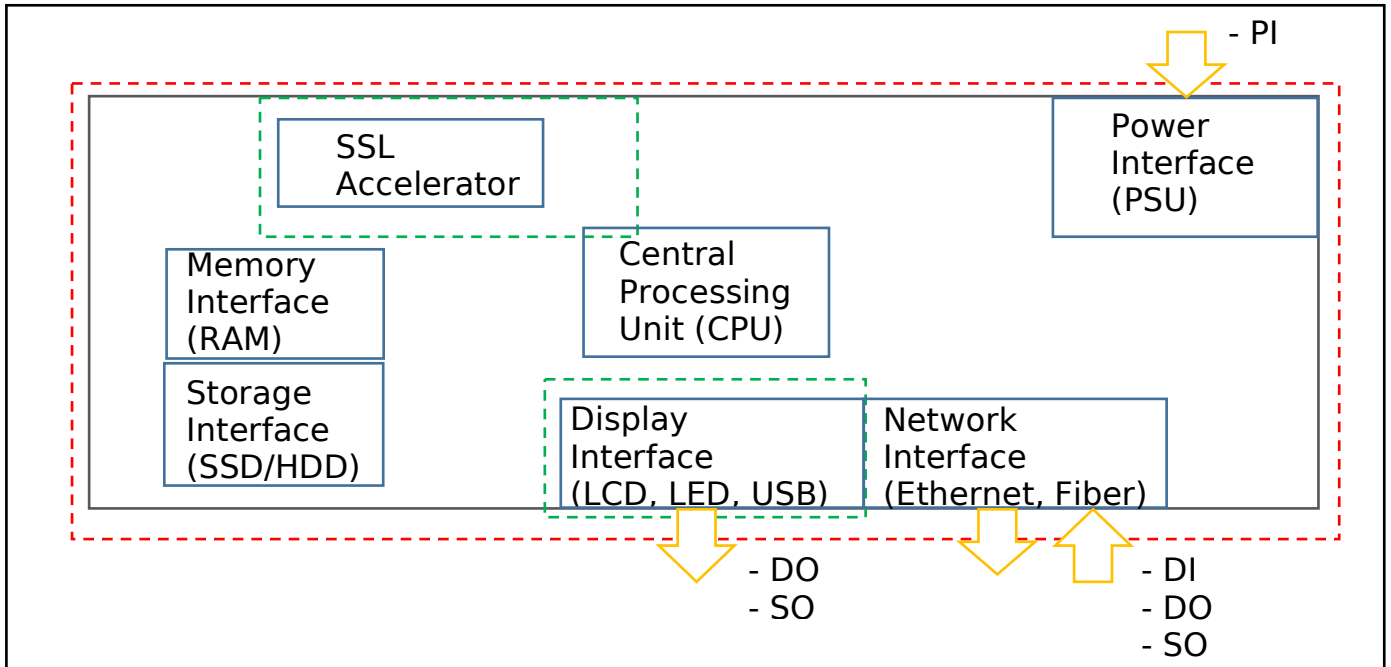
Algorithm	Usage	Notes
DSA		using any key size and SHA variant
ECDSA		FIPS 186-4 using curves other than P-256 and P-384, all SHA sizes
		FIPS 186-4 using curves P-256 and P-384 signature generation: SHA-1, SHA-224, SHA-512 signature verification: SHA-224 and SHA-512
SHA-224 SHA-512 MD5 SM3	Message Digest	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 5 - Non-Approved and Non-Compliant Cryptographic 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 block diagram below shows the module, its interfaces with the operational environment and the delimitation of its logical boundary. Figure 1 also depicts 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 6 - Ports and Interfaces*.

Figure 1 - Hardware 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 following table 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 QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 100Gbps.
Data Output	Network Interface Display Interface	Depending on module, the network interface consists of SFP, SFP+, and QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 100Gbps. 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 API which control system state (e.g. reset system, power-off system).
Status Output	Display Interface	Depending on model, the display interface can consist of a LCD display, LEDs, and/or output to STDOUT which provides system status information.
Power Input	Power Interface	PSU

Table 6 - Ports and Interfaces

Figure 4 and Figure 7 show the various platforms on which the module was tested. Please use the images to familiarize yourself with the devices.



Figure 2 - BIG-IP i4600 and BIG-IP i4800



Figure 3 - BIG-IP i5600, BIG-IP i5800 and BIG-IP i5820-DF



Figure 4 - BIG-IP i7600, BIG-IP i7800 and BIG-IP i7820-DF



Figure 5 - BIG-IP i10600, BIG-IP i10800 and BIG-IP i11600-DS, BIG-IP i11800-DS



Figure 6 - BIG-IP i15600, BIG-IP i15800



Figure 7 - BIG-IP 10350v-F



Figure 8 - VIPRION B2250



Figure 9 - VIPRION B4450

3 Roles, Services and Authentication

3.1 Roles

The module supports roles-based authentication. The FIPS 140-2 roles are defined below and purpose of role are described in the Table 7.

- **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 User role is mapped to multiple BIG-IP roles which are responsible for different components of the system (e.g. auditing, certificate and key management, user management, etc.). The User can access the module through Command Line Interface (CLI) or Web Interface. 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. This entity performs module installation and initialization. This role has full access to the system and has the ability to create, delete, and manage other User roles on the system.

The module supports concurrent operators belonging to different roles (one CO role 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:

- **CLI:** The module offers a CLI called traffic management shell (tmsh) which is accessed remotely using the SSHv2 secured session over the Ethernet ports.
- **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. Power-cycling the system requires the authentication credentials to be re-entered. Authentication data is protected against unauthorized disclosure, modification and substitution by the Operating System.

Additionally, 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 system. This role has complete access to all objects on the system. Entities with this role cannot have other roles on the system.
User	Auditor	Entity who can view all configuration data on the system, 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.
	Resource Manager	Grants a user access to all objects on the system 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 system 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 system.
	User Manager	Entity who manages BIG-IP crypto officer and user accounts. Create, Modify, view, Enable or Disable terminal access for any user account.

Table 7 - 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)	<p>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)</p> <p>Assuming a worst-case scenario where the password contains four digits, one ASCII lowercase letter and 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 $1/1,000,000$.</p>	<p>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 $1/100,000$.</p>
	Signature Verification (CLI only)	<p>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 $1/1,000,000$.</p>	<p>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 $1/100,000$.</p>
User	Password based (CLI and Web Interface)	<p>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)</p> <p>Assuming a worst-case scenario where the password contains four digits, one ASCII lowercase letter and 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 $1/1,000,000$.</p>	<p>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 $1/100,000$.</p>

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 8 - 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 9 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 9 - Non-Authenticated Services

Table 10 lists the services for the management of the module available in FIPS mode of operation which are only available after the authentication has succeeded. The Services, the Roles that can request the Service and the CSPs involved and how the CSPs are accessed (Read / 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 all User accounts	N/A	N/A	✓	User Manager Resource Manager Auditor
Create additional User	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 others password	password	W	✓	User Manager
Configure Password Policy Set password policy features	N/A	N/A	✓	N/A
Certificate and Keys Management Services				
Create / Delete SSL Certificate 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
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 Certificate Display / log 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 SSL Certificate	N/A	N/A	✓	Certificate Manager
Export Certificate File	N/A	N/A	✓	Certificate Manager

Service / Description	Keys-CSPs	Access Type (R, W, Z)	Authorized Role	
			Crypto Officer	User
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 Set policy rules, and address-lists for use by firewall rules.	N/A	N/A	✓	Firewall Manager
Show firewall state Display the current system-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 System Audit log Display logs/files of configuration changes	N/A	N/A	✓	Auditor Resource Manager
Export Analytics Logs system	N/A	N/A	✓	Auditor
Enable/ Disable Audit	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	✓	Resource Manager
	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

Service / Description	Keys-CSPs	Access Type (R, W, Z)	Authorized Role	
			Crypto Officer	User
Configure nodes create, modify, view, delete nodes	N/A	N/A	✓	Firewall Manager Resource Manager
Configure iRules create, modify, view, 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 system zeroization	All CSPs in Table 15	W, Z	✓	N/A

Table 10 - Authenticated Management Services in FIPS mode of operation

Table 11 lists the TLS and SSH crypto Services available in FIPS mode of operation, the Roles that can request the Service, the algorithms and the CSPs involved and how the CSPs are accessed (Read/Write/Zeroize - R, W, Z).

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type	Interface	
					Data Plane	Control Plane
SSH Services						
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	SSH RSA key pair, SSH ECDSA key pair	R		Yes
	Key Exchange: EC Diffie-Hellman		SSH EC Diffie-Hellman key pair, SSH shared secret	R, W		
	Key Derivation: [SP800-135] SSH KDF		SSH shared secret Derived SSH session key (AES, HMAC)	R, W		
Maintain SSH Session	Data Encryption and Decryption: AES (CBC mode)	User CO	Derived SSH session key (AES)	R		Yes
	Data Integrity (MAC): HMAC with SHA-1		Derived SSH session 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 ECDH 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 11 - Crypto Services in FIPS mode of operation

Table 12 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 5 row <i>Digital Signature Generation and Verification</i>
		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		

Service	Role	Usage/Notes
Establish SSH session	User/ CO	Signature generation and verification using: DSA, RSA, ECDSA algorithms listed in Table 5 row <i>Digital Signature Generation and Verification</i> 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 system through REST using non-approved crypto from Bouncy Castle
Configuration using SNMP		Management of the module via SNMP is not approved.

Table 12 - Services in non-FIPS mode of operation

4 Physical Security

All of the modules listed in Table 1 are enclosed in a hard-metallic production grade case that provides obscurity and prevents visual inspection of internal components. Each module 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 that the modules have not been tampered with. In the event that the tamper evident labels require replacement, a kit providing 25 tamper labels is available for purchase (P/N: F5-ADD-BIG-FIPS140). The Crypto Officer shall be responsible for the storage of the label kits.

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 13 - Inspection of Tamper Evident Labels

4.1 Tamper Label Placement

The pictures below show the location of all tamper evident labels for each hardware appliances listed in Table 1. Label application instructions are provided in section 8.2 Crypto-office guidance

Hardware Appliance	# of Tamper Labels	Hardware Appliance	# of Tamper Labels
BIG-IP i4600, BIG-IP i4800	4	BIG-IP i15600 BIG-IP i15800	4
BIG-IP i5600, BIG-IP i5800 BIG-IP i5820-DF	3	BIG-IP 10350v-F	4
BIG-IP i7600 BIG-IP i7800 BIG-IP i7820-DF	4	VIPRION B2250	6
BIG-IP i10600 BIG-IP i10800	4	VIPRION B4450	5
BIG-IP i11600-DS BIG-IP i11800-DS	4	-	-

Table 14 - Number of Tamper Evident Labels per hardware appliance

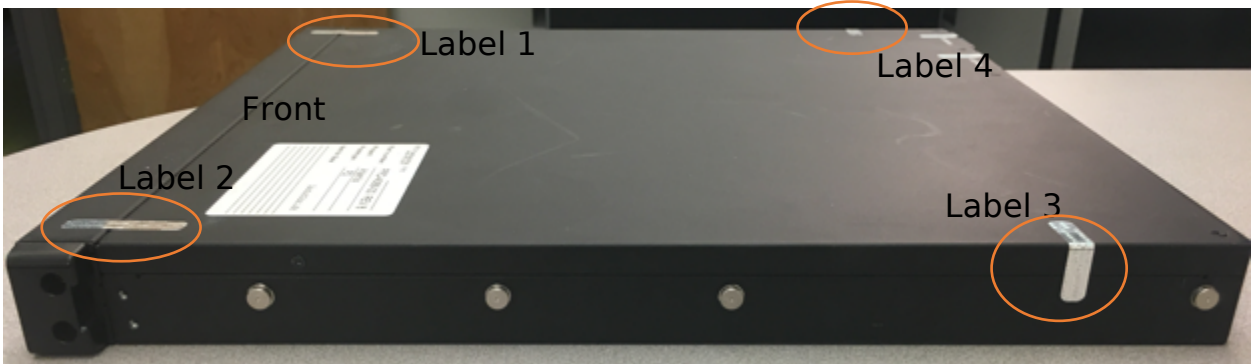


Figure 10 - Tamper labels on BIG-IP i4600 and BIG-IP i4800 (4 of 4 tamper labels)

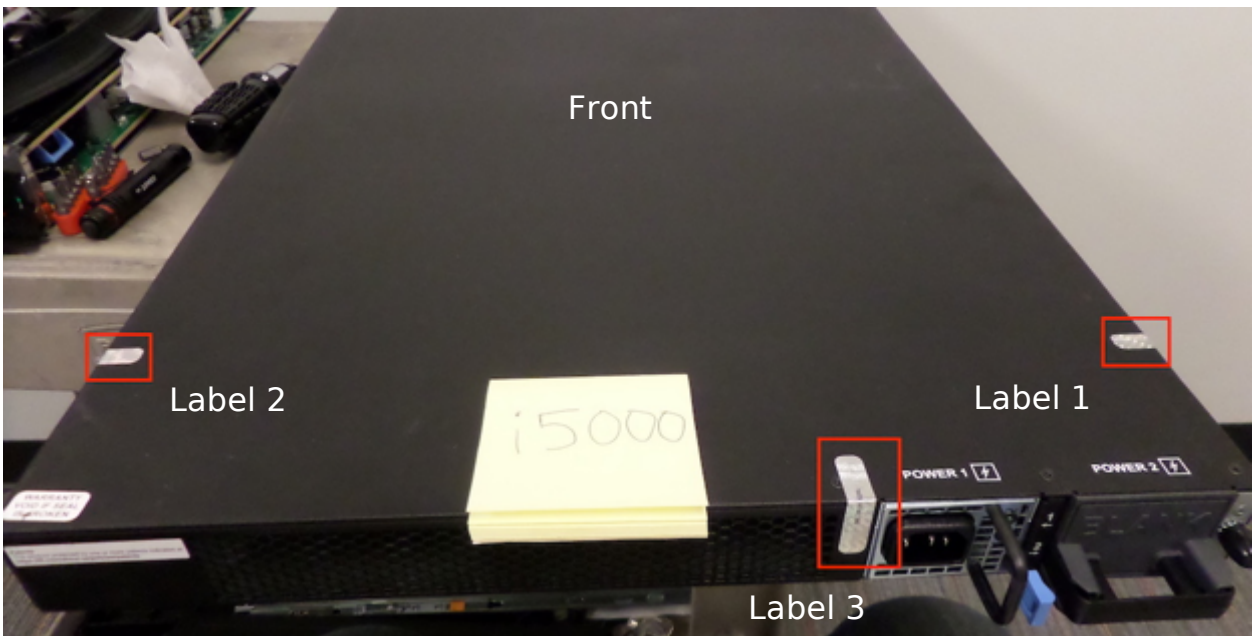


Figure 11 - Tamper labels on BIG-IP i5600, BIG-IP i5800 and BIG-IP i5820-DF (3 of 3 tamper labels)

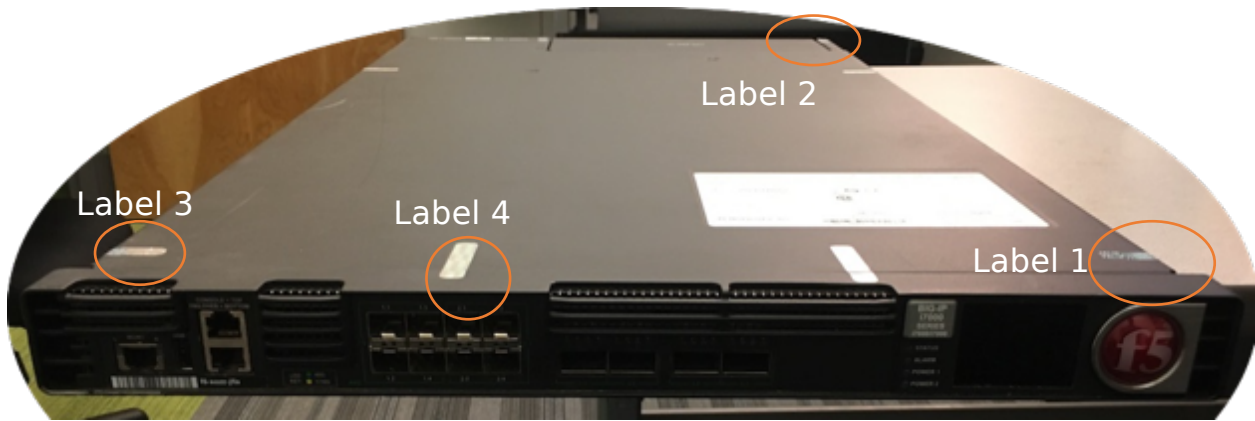


Figure 12 - Tamper labels on BIG-IP i7600, BIG-IP i7800 and BIG-IP i7820-DF with tamper labels shown on the front side of the platforms -label 2- on the opposite lateral sides of the platform -labels 1,3 and on the ventilation fan tray that allows access to SSDs- label 4. The PSU housings are opaque to internal components and do not need to be secured with evident labels.

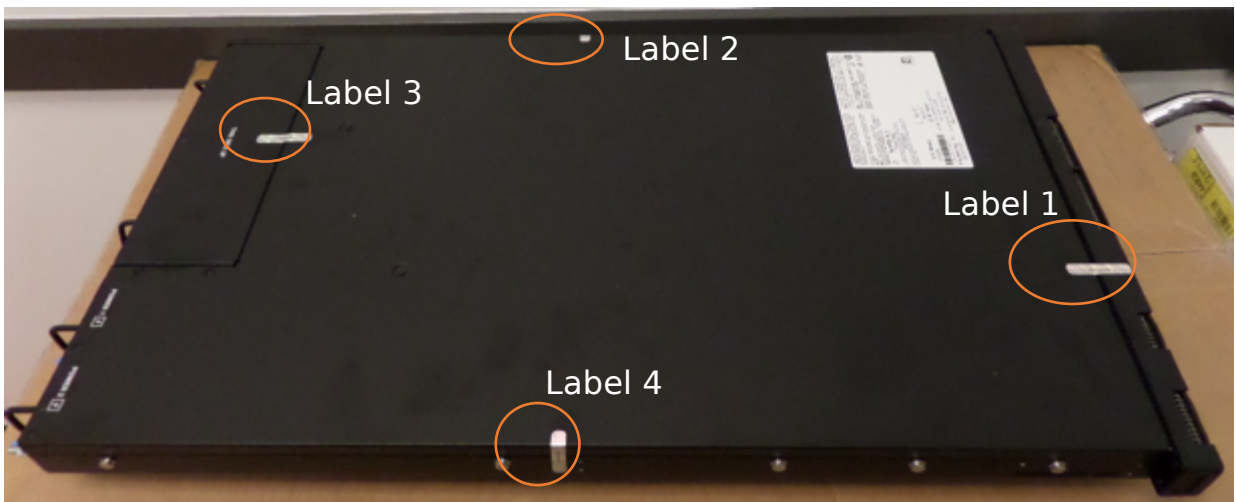


Figure 13 - Tamper labels on BIG-IP i10800, BIG-IP i10600 and BIG-IP i11600-DS, BIG-IP i11800-DS (4 tamper labels shown)



Figure 14 - Tamper labels on BIG-IP i15600, BIG-IP i15800. Left: Front and side tamper labels (3/ 3 labels shown). Right: Label 4 to mark with evidence the unauthorized removal of the fan tray (replaceable item) that gives access to replaceable storage drives. (1 tamper label shown circled in orange)

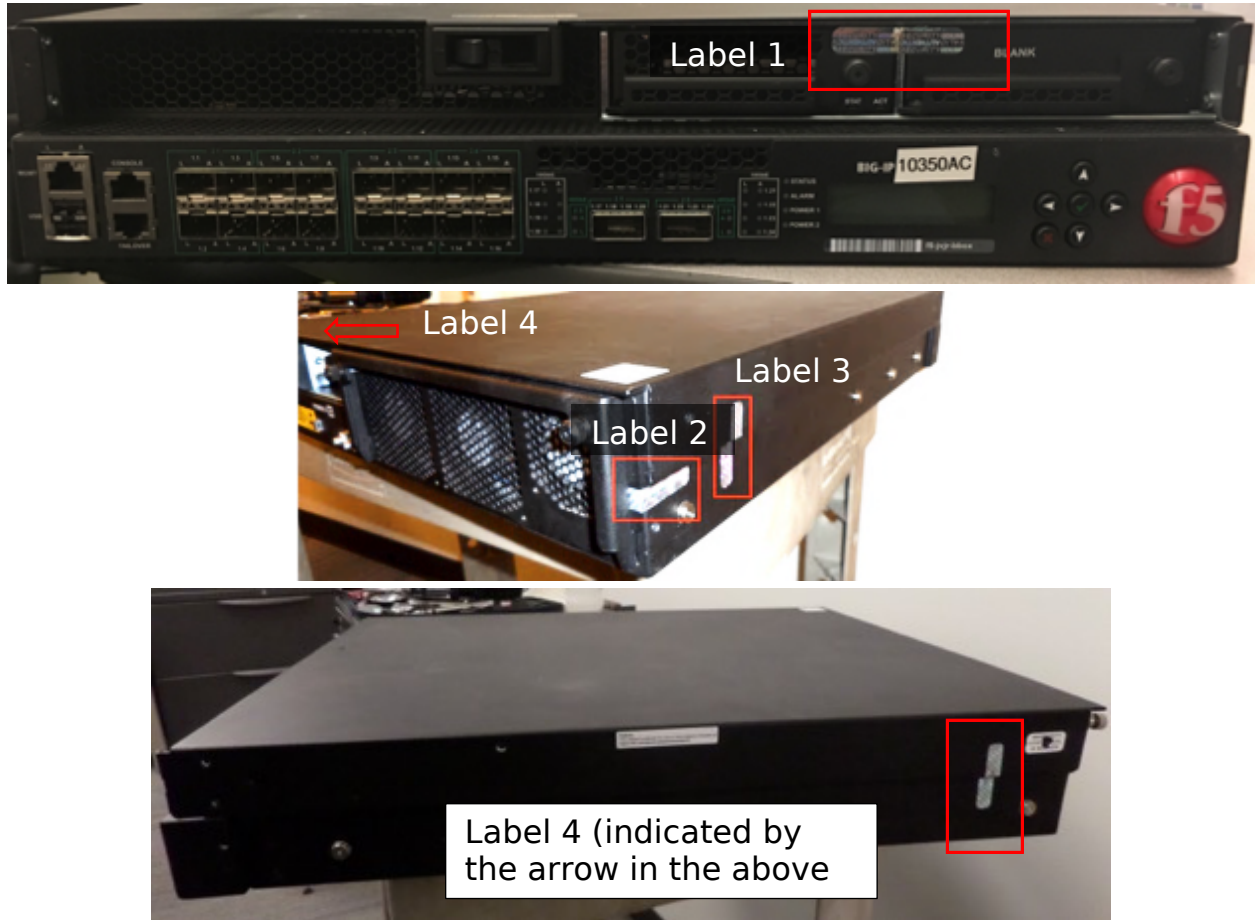


Figure 15 - Tamper labels on BIG-IP 10350v-F. Top: BIG-IP 10350v-F with faceplate from Picture Table 1 removed and the tamper label 1 affixed to secure the housing for externally-accessible storage drives. Middle, Bottom: tamper labels shown at the intersection between cover and chassis (2 opposite sides of the platform -labels 3 and 4- and front -label 2-).



Figure 16 - Tamper labels on VIPRION B2250 in chassis (1 of 6 tamper labels shown)

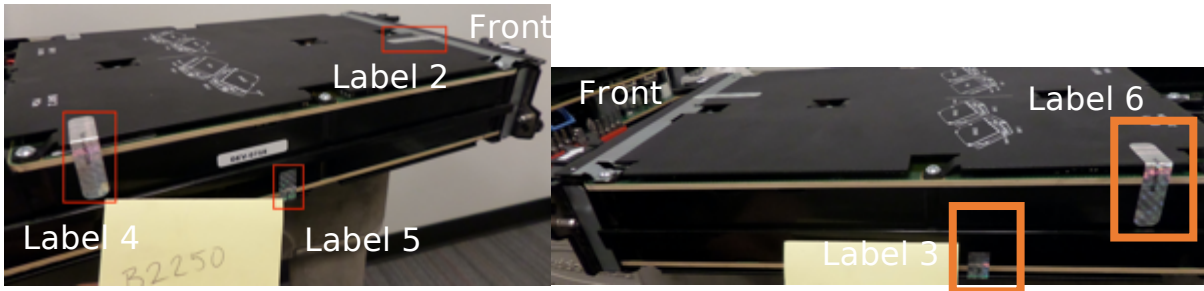


Figure 17 - Tamper labels on top view VIPRION B2250, and two sides VIPRION B2250 (5 of 6 tamper labels shown)

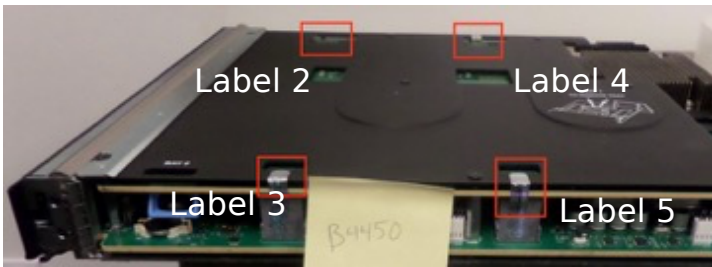


Figure 18 - Tamper labels on VIPRION B4450 top-view (4 of 5 tamper labels shown)



Figure 19 - Tamper labels on VIPRION B4450 in chassis (1 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

Table 15 summarizes the key and CSPs that are used by the cryptographic services implemented in the module. Sizes for the listed keys are given in Table 3 and Table 4 section 1.3.

Key / CSPs	Generation	Storage	Zeroization
Entropy input string	Obtained from ENT (NP)	RAM	Zeroized by device reboot
DRBG seed, V and Key values	Derived from entropy string as defined by [SP800-90ARev1]	RAM	
TLS RSA key pair	Generated using [FIPS 186-4] Key generation method. 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 key pair		RAM	Zeroized by closing TLS session or by rebooting the device.
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 device.
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 device.
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. The random value used in the key generation is generated using [SP800-90ARev1] DRBG.	RAM	
SSH RSA 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 15 - Life cycle of CSPs

6.1 Key Generation

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

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per [SP800-133r2] (vendor affirmed).

The module does not implement symmetric key generation as an explicit service. The HMAC and AES symmetric keys are derived from shared secret by applying [SP 800-135] as part of the TLS/SSH protocols. The scenario maps to the [SP 800-133r2] section 6.2.1 *Symmetric keys generated using Key Agreement Scheme*.

6.2 Key Establishment

The module provides the following key establishment services:

- RSA Key wrapping scheme 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 KDF.
- [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 approved authenticated encryption mode (i.e. AES-GCM) provides 128 or 256 bits of encryption strength (AES-GCM Certs. #A1350 and #A1351) for TLS protocol.
- [SP 800-38F] key wrapping using a combination of approved AES encryption and HMAC authentication method provides 128 or 256 bits of encryption strength (AES-CBC and HMAC Certs. #A1350 and #A1351) 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. #A1351) 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, any key or data transfer performed thereafter is protected by AES encryption.

6.4 Key / CSP Storage

As shown in Table 15 the keys stored in the volatile memory (RAM) in plaintext form and are destroyed when released by the appropriate zeroization calls or when the system is rebooted. The keys stored in plaintext in non-volatile memory (SSD/HDD) are static and will remain on the system across power cycle and are only accessible to the authenticated administrator.

6.5 Key / CSP Zeroization

The zeroization methods listed in Table 15, 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 device) 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. 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 the health tests for the DRBG as defined per section 11.3 of [SP800-90ARev1].

The module uses a SP800-90B compliant non-physical entropy source (ENT (NP)) to seed the DRBG and provides at least 256 bits of entropy. 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 device is booted 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 clear the error states.

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 system enters "Halt Error" state and the device 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 GCM mode and 128-bit key KAT of AES encryption and decryption performed separately with ECB mode and 128-bit key

Algorithm	Test
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
SSC for the KAS	“Z” computation KAT with P-256 curve
[SP800-135] KDF	SSH KAT TLS1.0/1.1 and TLS1.2 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
• Data Plane Self-Tests	
AES	KAT of AES encryption with GCM mode and 128-bit key KAT of AES encryption /decryption performed 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, SHA-256
SSC	“Z” computation KAT with P-256 curve
CTR_DRBG	Covered by Control Plane Self-Tests. (Data Plane makes use of the same DRBG implementation provided by Control Plane)
[SP800-135] KDF	TLS1.0/1.1 and TLS1.2 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 16 – 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 system 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 PCT tests, the module reboots and enters into the “Halt Error” state.
- If the ENT (NP) SP800-90B health tests fail, then the module moves into the “Health Test Error” state.

In any of the error states, any data output or cryptographic operations are prohibited. 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 17 - 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 should be completed by the Crypto Officer prior to access to the device is allowed.

8.2.1 Installing Tamper Evident Labels

Before the device 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 should 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 Device

Follow the instructions in the "*BIG-IP System: Initial Configuration*" guide for the initial setup and configuration of the device.

- 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 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.

8.2.4 Additional Guidance

The Crypto Officer should 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 system are not allowed.
- Serial port console should be disabled after the initial power on and communications setup of the hardware.
- On the i11800-DS device, the Cavium Nitrox-V must be disabled using `lspci | grep -i encryption | awk '{print "device exclude " $1;}' > tmm_init.tcl` command since full support is not available:
- 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.
- The Single DH should be turned ON for the platform GUI.

8.2.5 Version Configuration

Once the device is installed, licensed and configured, the Crypto Officer should confirm that the system is installed and licensed correctly.

8.2.5.1 Version Confirmation

The Crypto Officer should run the command "tmsh show sys version", then confirm that the provided version matches the validated version shown in Table 1 - Tested Modules. 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.

8.2.5.2 License Confirmation

The FIPS validated module activation requires installation of the license referred as 'FIPS license'. The Crypto Officer should 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 11 – Crypto Services in FIPS mode of operation lists the FIPS approved services and Table 12 – Services in non-FIPS mode of operation lists the non-FIPS approved services. Using the non-FIPS approved algorithm or mode in Table 5 – Non-Approved and Non-Compliant Cryptographic Algorithms/Modes means that the module operates in non-FIPS Approved mode for the particular session of a particular service.

AES-GCM IV is constructed in accordance with SP800-38D in compliance with IG A.5 scenario 1. 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. 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 follows [RFC 5288] 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
APT	Adaptive Proportion Test (a 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
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
ENT (NP)	non-physical Entropy Source
OFB	Output Feedback
RCT	Repetition Count Test (a 90B continuous health test)
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
XTS	XEX-based Tweaked-codebook mode with cipher text stealing

Appendix B. Selection of References

FIPS140-2	FIPS PUB 140-2 - Security Requirements For Cryptographic Modules May 2001 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
FIPS140-2_IG	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf
FIPS180-4	Secure Hash Standard (SHS) Aug 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS186-4	Digital Signature Standard (DSS) July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS197	Advanced Encryption Standard November 2001 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
FIPS198-1	The Keyed Hash Message Authentication Code (HMAC) July 2008 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf
PKCS#1	Public Key Cryptography Standards (PKCS) #1: RSA Cryptography https://tools.ietf.org/html/rfc8017
SP800-38A	NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf
SP800-38D	NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
SP800-56A Rev3	NIST Special Publication 800-56A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Apr 2018, rev3 https://doi.org/10.6028/NIST.SP.800-56Ar3
SP800-90A	NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators Jun 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

SP800-131A NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
Mar 2019
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf>