TippingPoint®

HEWLETT PACKARD ENTERPRISE

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

TippingPoint Intrusion Prevention System

Hardware Versions: S660N and S1400N
Firmware Version: 3.8.2

Document Version: 3.2
Revision Date: 01/04/2016

FIPS 140-2 Non-Proprietary Security Policy

TippingPoint Intrusion Prevention System

Contents

List of Figures

List of Tables

1. Introduction

This document is a non-proprietary Cryptographic Module Security Policy for the TippingPoint Intrusion Prevention System (IPS) models S660N and S1400N. These models should be operated with the 3.8.2 firmware version for compliance with the security policy described herein. Using other versions of firmware will remove the module from the FIPS approved mode of operation.

This Security Policy may freely be reproduced and distributed in its entirety (without modification).

Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the U.S. and Canadian Governments' requirements for cryptographic modules. The following pages describe how TippingPoint IPS meets these requirements and how to use the IPS in a mode of operation compliant with FIPS 140-2. This policy was prepared as part of the Overall Level 1 FIPS 140-2 validation of the TippingPoint Intrusion Prevention System.

More information about FIPS 140-2 and the Cryptographic Module Validation Program (CMVP) is available at the website of the National Institute of Standards and Technology (NIST): http://csrc.nist.gov/groups/STM/cmvp/index.html.

In this document, the TippingPoint Intrusion Prevention System is referred to as the *IPS*, the *module*, or the *device*.

1.1. Purpose

This document covers the secure operation of the TippingPoint IPS appliances including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner.

1.2 References

This Security Policy deals specifically with the operation and implementation of the module in the technical terms of the FIPS 140-2 standard. Additional information on the module can be found on the TippingPoint website.

1.3 Definitions and Acronyms

This Security Policy uses the following definitions and acronyms.

Table 1: Definitions and Acronyms

Term/Acronym	Description
AES	Advanced Encryption Standard
CF	Compact Flash
CLI	Command Line Interface
CSP	Critical Security Parameter

DES	Data Encryption Standard
DH	Diffie Hellman
DRBG	Deterministic Random Bit Generator
DRNG	Deterministic Random Number Generator
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention System
LCD	Liquid Crystal Display
LSM	Local Security Manager
MD5	Message Digest 5
RNG	Random Number Generator
RSA	Public Key encryption developed by RSA Data Security, Inc. (Rivest, Shamir and Adleman)
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SMS	Security Management System
SRDI	Security Relevant Data Item
SSH	Secure Shell
Triple-DES	Triple Data Encryption Standard
TLS	Transport Layer Security
TP	TippingPoint
XFP	10 Gigabit Small Form Factor Pluggable
ZPHA	Zero Power High Availability. ZPHA is a mechanism which allows IPS network traffic intended for the module’s monitoring ports to continue to flow when it loses power.

2. Module Specifications

2.1 Overview

The TippingPoint IPS operates in-line in the network, blocking malicious and unwanted traffic, while allowing good traffic to pass unimpeded. In fact, the module optimizes the performance of good traffic by continually cleansing the network and prioritizing applications that are mission critical.

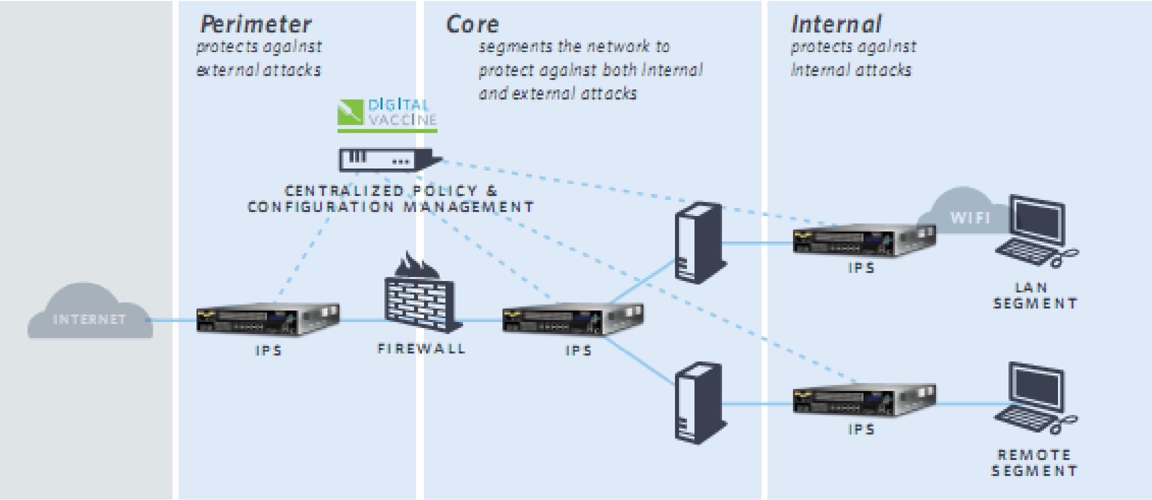
Perimeter
protects against external attacks
Core
segments the network to protect against both internal and external attacks
Internal
protects against internal attacks
DIGITAL VACCINE
CENTRALIZED POLICY & CONFIGURATION MANAGEMENT
INTERNET
IPS
FIREWALL
IPS
WIFI
IPS
LAN SEGMENT
IPS
REMOTE SEGMENT

Figure 1: TippingPoint IPS Deployment in a Network

The TippingPoint IPS is deployed seamlessly into the network and immediately begins filtering out malicious and unwanted traffic. Its switch-like performance characteristics allow it to be placed in-line at the perimeter, on internal network segments, at the core, and at remote site locations. These powerful enforcement points can be centrally controlled to institute and enforce business-wide security policies, allowing the TippingPoint IPS to see all network traffic and protect against external as well as internal attacks.

TippingPoint solutions decrease IT security cost by eliminating ad-hoc patching and alert response, while simultaneously increasing IT productivity and profitability through bandwidth savings and protection of critical applications.

2.2 Security Level

When operated in the FIPS approved mode of operation (denoted 'Full-FIPS' mode on the appliance), the TippingPoint IPS Cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

2.3 Physical Characteristics

From a FIPS 140-2 perspective, each TippingPoint IPS model is considered to be a multiple-chip standalone hardware module using production-grade components contained within an opaque, hard enclosure made of production-grade steel.

The S660N and S1400N IPS models should be operated with the 3.8.2 firmware version.

The IPS module only allows the installation of new firmware signed by a TippingPoint private key so it has a limited operational environment.

The IPS module is available in the following physical configurations:

1. S660N and S1400N (same physical configuration)

The module configurations are shown in the picture below:

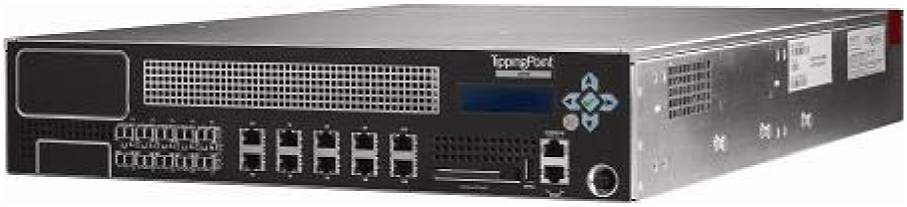

Figure 2: TippingPoint S660N/S1400N

The module configuration is listed in the Table below:

Table 3: Hardware Comparison

IPS Model	Removable components	Dimension (H*W*D) (inches)	Monitoring Ports (excluded)	Management Interfaces	Inspection Through-put
S660N	Fans, power supplies, external CF, SFP transceivers	3.42*16.8*24 (2U rack-mountable)	5 segments (10 ports) RJ-45 10/100/1000 Ethernet (Copper) ; 5 segments (10 ports) 1GbE SFP	1 10/100/1000 GbE Copper port, 1 RJ-45 Console port, 1 LCD and Keypad	750Mbps
S1400N					1.5Gbps

2.4 Cryptographic Boundary

The cryptographic boundary of the module is the module's external hard-metal enclosure that forms the physical perimeter of the module. The cryptographic boundary includes all components within the hard metal enclosure of the module.

2.5 Excluded Components

The following module components are excluded from FIPS 140-2 requirements:

1. Monitoring Ports

The module may have different types of monitoring ports (i.e. Copper or SFP) depending on the module configuration used. Each of the above physical configurations of the module has 2 ports per segment, which are used for the IPS functionality. One of the ports in a segment is typically used for the internal protected network while the other port is used for the external unprotected network. These ports are used only for the network data that is monitored for intrusion prevention services, and these ports are not associated with any cryptographic processes, keys or CSPs. The monitoring ports can never input or output any cryptographic keys, CSPs, or any FIPS-relevant data. Thus, these ports cannot affect the security of the module and are excluded from FIPS 140-2 security requirements.

2. ZPHA Connector Port:

The module configurations have a ZPHA connector port which can be used to support an optional ZPHA Module. The ZPHA connector can accommodate only one ZPHA module at a time. These ZPHA modules have monitoring ports which can be connected to external networks and to the IPS module's monitoring ports using external network cables. This enables the module to support the Zero Power High Availability (ZPHA) mechanism, which allows IPS network traffic to continue to flow when the box loses power. The ZPHA connector and the ports supported by the ZPHA modules are not associated with any management data, cryptographic services, keys or CSPs. The ZPHA connector can never compromise the IPS module’s security and is excluded from FIPS 140-2 security requirements.

2.6 Ports and Interfaces

Each IPS model provides a management port and a console port, which carry all of the module’s cryptographic data, keys and CSPs.

COMPACT FLASH PORT:
The module configurations S660N and S1400N have an external compact flash port located on the front side of the module. The compact flash can be used only to store logs and other system data. No cryptographic keys, CSPs, or security-relevant management data can ever be input or output using this external compact flash.

The module configurations S660N and S1400N have only one USB port that is labeled “ZPHA” on the front side of the module body. This port is only used to provide power to an external ZPHA appliance. There is no other use of this port and it is not associated with any cryptography, keys, CSPs or security-relevant data.

The following table indicates the mapping of the module’s physical ports to the FIPS 140-2 logical interfaces.

Table 4: FIPS 140-2 Interfaces and the Corresponding Module’s Physical Ports

FIPS 140-2 Logical Interface	Module’s Physical Port
Data Input	Ethernet Management Port
	RJ-45 Console Port
	Compact Flash Port
Data Output	Ethernet Management Port
	RJ-45 Console Port
	Compact Flash Port
Control Input	Ethernet Management Port
	RJ-45 Console Port
	Power/Reset Button/Switch
	LCD Keypad
Status Output	Ethernet Management Port
	RJ-45 Console Port
	LCD Screen
	LEDs
	Compact Flash Port
Power Interface	Power Port
	USB Port

2.7 Modes of Operation

The module can be operated in a FIPS-approved mode or in a non-FIPS mode. The module supports 3 modes of operation: Disable, Crypto, and Full. Only the ‘Full’ FIPS mode on the module is considered as the FIPS Approved mode of operation. The ‘Disable’ mode and the ‘Crypto’ mode on the module are considered as non-FIPS modes of operation.

The cryptographic algorithms allowed by the module in the Approved Full-FIPS mode of operation are indicated in Table 8 of this document. The Cryptographic Keys, CSPs, and SRDIs of the module in an Approved mode of operation are described in Table 10 of this document. The rules and procedures followed and enforced by the module in the Approved mode of operation are described in Section 4 of this document.

3. Roles, Services, and Authentication

3.1. Authentication Mechanisms and Strength

An operator can authenticate and access the module in any one of the following ways:

- CLI over Console Port
- CLI via SSH over Management Port
- CLI via Telnet over Management Port
- LSM (HTTP or HTTPS) over Management Port. LSM stands for the Local Security Manager, which offers a Web-based GUI for managing one IPS device. LSM provides a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides reports to monitor the device traffic, triggered filters, and packet statistics. HTTP is disabled in FIPS mode and HTTPS provides TLS protection.
- Using the TippingPoint SMS Client GUI via TLS over Management Port for allowing management of the IPS module by the SMS. SMS stands for the Security Management System, which is a central management point for managing different TippingPoint appliances, monitoring events and scheduling reports. A single SMS can be used to monitor and manage multiple IPS devices. This authentication is required for enabling the SMS management.
- Using a TippingPoint SMS as a remote authentication server. This is possible only when the IPS is already being managed by an SMS. Remote authentication can only be used with CLI and LSM. The remote authentication data is always protected by TLS.
- Using RADIUS for remote authentication (disallowed by policy when in Full FIPS mode).
- Using TACACS+ for remote authentication (disallowed by policy when in Full FIPS mode).

Telnet and HTTP are disabled by default and cannot be enabled while in Full FIPS mode. SSH and HTTPS must be used instead.

RADIUS and TACACS+ authentication support is disallowed by policy so should not be enabled when in Full FIPS mode.

The TippingPoint IPS supports password authentication for all users. A user must specify a name and password when authenticating to the IPS through LSM, through the CLI, using the SMS Client, or using an SMS as a remote authentication server.

AUTHENTICATION STRENGTH:

When authenticating through the CLI, through LSM, or using the SMS client to an IPS in Full FIPS mode with remote authentication disabled, the IPS does the enforcement of user name and password restrictions. The IPS requires usernames with a minimum of 6 characters and passwords with a minimum of 8 characters. In the default configuration, there is no restriction on what characters can be in the password. Thus, there are 95^8 (i.e. 6.6*10^15) possible passwords of the minimum length from the set of all displayable ASCII characters including space. The odds of randomly guessing a password of the minimum length would thus be 1 in 6.6*10^15 which is much less than 1 in 1,000,000. Thus, it meets the FIPS requirement.

The IPS has a password configuration option that requires passwords to have at least 2 letters (i.e. 52 possible for each), 1 number (i.e. 10 possible), and 1 non-alphanumeric character (i.e. 95-52-10=33 possible). This would reduce the number of possible passwords from the default settings. Assuming a minimum password length and fixed positions (but not values) for the restrictive character classes, the number of possible passwords is 52*52*10*33*(95^4) = 7.3*10^13. The odds of randomly guessing a password would thus be 1 in 7.3*10^13 which is much less than 1 in 1,000,000. Since the positions of the required character classes are not fixed, the number of possible passwords of the minimum length is larger. Thus the actual odds are even lower.

When authenticating through the CLI or through LSM to an IPS in Full FIPS mode with remote authentication enabled, the SMS by default does the enforcement of user name and password restrictions. For maintaining FIPS compliance while using remote authentication with an IPS in Full FIPS mode, the SMS must be configured to use the highest setting (i.e. level 2) for users and passwords. The SMS level 2 setting requires a minimum of 6 character usernames. This setting also requires a minimum of 8 character passwords with no spaces where 2 must be letters (i.e. 52 possible for each), 1 must be numeric (i.e. 10 possible), and 1 must be non-alphanumeric (i.e. 94-52-10=32 possible). Assuming a minimum password length and fixed positions (but not values) for the restrictive character classes, the number of possible passwords is 52*52*10*32*(94^4) = 6.7*10^13. The odds of randomly guessing a password would thus be 1 in 6.7*10^13 which is much less than 1 in 1,000,000. Since the positions of the required character classes are not fixed, the number of possible passwords of the minimum length is larger. Thus the actual odds are even lower.

When authenticating through the CLI or through LSM to an IPS in Full FIPS mode with remote authentication disabled, the IPS does the enforcement of the number of unsuccessful login attempts allowed within a given period. In the default configuration, a user account is locked for 5 minutes after 5 failed login attempts for that user. Thus the odds of randomly guessing a password with retries within one minute is 5 times the odds discussed above (i.e. 1 in 7.3*10^13 in the largest odds case) for IPS enforcement resulting in odds of about 1 in 1.4*10^13, which is much less than 1 in 100,000, and thus meets the FIPS requirement. The maximum number of retries can be configured up to 10, which would result in 10 times the odds discussed above, which results in odds of about 1 in 7.3*10^12, which is still much less than 1 in 100,000. To maintain FIPS compliance, the user must not disable the configuration for account lockout on login failure or configure the lockout time to less than 1 minute.

When authenticating to an IPS in Full FIPS mode using the SMS client or through the CLI or LSM with remote authentication enabled, the fastest transfer speed is 1 Gbps over the management port. 1 Gbps corresponds to 7.5*10^9 bytes/min. For any of these scenarios, both the user name and password are sent on each login attempt. The minimum for this will be 14 bytes (6 character username plus 8 character password). Thus the maximum logins per minute would be 7.5*10^9 / 14 = 5.4*10^8 logins/min. The odds for a successful login on repeated tries within a minute would thus be 5.4*10^8 times the odds for one login. When the IPS is enforcing the password restrictions (i.e. using the largest odds case of 1 in 7.3*10^13), the resulting retry odds are about 1 in 135,000 which is less than 1 in 100,000 as required by FIPS. When SMS is enforcing the password restrictions (i.e. using odds of 1 in 6.7*10^13), the resulting retry odds are about 1 in 120,000 which also meets the FIPS requirement. Note that the actual odds for these scenarios is even lower due to the actual odds on one attempt being lower than the estimates (see above) and due to overhead for sending the login information that is not included in the estimates.

3.2. Roles

For each of the above access methods, the TippingPoint IPS supports an identity-based authentication mechanism, where each user has an individually identified Username and Password. An access level is associated with each user. An access level is associated with each user. There are 3 user access levels and their corresponding FIPS roles are shown in the table below. A user, who sets up and performs the first-time initialization of the module, is implicitly assigned a Super-User Crypto-Officer role.

Table 5: Roles and Descriptions

User Access Level	Description	FIPS Role	Type of Authenti-cation	Authenti-cation Data
Operator	Can login to the CLI and LSM but primarily has read-only access to the configuration settings. The only CSP an operator can modify is his own password.	User	Identity-based	Username and Password
Administrator	Can login to the CLI and LSM and modify some configuration settings. An administrator can modify his own password, can load a new TLS RSA key pair over TLS, and can perform	Crypto-Officer	Identity-based	Username and Password

	software upgrades to the module.			
Super-User	Can login to the CLI and LSM and modify all configuration settings. Only a Super-User can login to the SMS to manage multiple IPS modules. Only a super-user can add and delete users and modify any user's password and access level. Also, only a super-user can configure the box for FIPS mode and do all key management.	Crypto-Officer	Identity-based	Username and Password

The IPS module does not have support for a maintenance role. The IPS module does not support bypass mode.

Concurrent Operators
The module allows up to 10 concurrently authenticated operators and rejects any additional authentication requests. In addition, at least one Super-User must remain in the module so the module does not allow the deletion of the last Super-User (Crypto-Officer).

3.3. Module Services

The table below shows the services provided by the IPS and the access level required to perform them.

Table 6: Module Services

Operator	Administrator	Super User	Service	Service Input	Service output	Notes
		Y	Enable Full-FIPS mode	None	None	Only applicable to non-FIPS modes. Not allowed to change mode once in full FIPS mode.
Y	Y	Y	View FIPS status	None	FIPS status, current authenticated	

					user information, logs.	
Y	Y	Y	Configure own password	Username and Password	None	
		Y	Configure any user’s password and access level	Username and password	None	
	Y	Y	Configure password restrictions and other user account settings for all users	New value of the setting option.	None	
		Y	Zeroize keys	None	None	Done by “fips keys delete” CLI command which requires reboot. The ephemeral keys are also always zeroized on a reboot (see reboot service below).
		Y	Generate new keys	None	None	Done by “fips keys generate” CLI command which requires reboot (see reboot service below). Some keys (e.g. SP800-90A CTR_DRBG SRDIs) are also regenerated on a reboot. The ephemeral TLS/SSH keys are generated during TLS/SSH session

						negotiation (see login services below).
	Y	Y	Install new TLS RSA key pair	New TLS RSA Key Pair encrypted with TLS session key	None	
	Y	Y	Reboot	None	None	Can also be done unauthenticated using the power/reset button or power cycling the box.
	Y	Y	Install or update new software	Software package signed by TippingPoint, TLS parameters, data and input	None if it succeeds and error message if it fails.	
			Perform FIPS power-up self-tests	None	None if all tests pass. If any test fails, log message is generated and module reboots.	Done automatically during initialization after reset or power cycle.
Y	Y	Y	Login to CLI	Username and password, SSH parameters, input and data (when using SSH)	CLI prompt if successful and login prompt if unsuccessful	
Y	Y	Y	Login to LSM	Username and password, TLS parameters, input and data (when using HTTPS)	LSM homepage if successful and login prompt if unsuccessful	
		Y	Login via SMS Client GUI for enabling	Username and password, TLS parameters,	System summary if successful and	

			central management	input and data	login prompt if unsuccessful	
Y	Y	Y	Remote authentication using SMS	Username and Password, TLS parameters, input and data	CLI prompt or LSM homepage, depending on the method used	Possible only if SMS is already managing the IPS.
	Y	Y	Configure non-FIPS related admin level settings	Corresponding setting values	None	
		Y	Configure non-FIPS related super-user level settings	Corresponding setting values	None	
Y	Y	Y	View non-FIPS related configuration	None	Non-FIPS related configuration information	
Y	Y	Y	View non-FIPS related status	None	Non-FIPS related status	
			Intrusion prevention functionality on the monitoring ports.	None	None	Done automatically based on the non-FIPS related configuration.

3.4. *Unauthenticated Services*

The IPS modules allow the following unauthenticated services:

Table 7: Unauthenticated Services

Service	Procedure	Service Inputs	Service Outputs
Power-off, halt or reboot the module	Using the power switch, power cycling the module, or using LCD and keypad	None	None
Perform power-up self-tests	Reboot the module	None	None
Zeroize ephemeral	Reboot the module	None	None

keys			
Show non-FIPS related information	Using LCD and keypad	None	Non-FIPS related information such as device temperature, serial number, current memory usage, etc. No key or CSP information is output by this service.
Configure non-FIPS related settings such as LCD backlight and contrast	Using LCD and keypad	None	None
Insert or Eject external compact flash	Using LCD and keypad or using eject switch	None	None

3.5 Non-FIPS Mode Services

The module supports the following non-FIPS mode services which shall not be used when operated in FIPS mode.

- SSH with Blowfish, MD5, and HMAC-MD5
- TLS with DES, RC2 and RC4
- SNMP v2

4. Secure Operation and Security Rules

This section describes the rules enforced in the module when operated in the FIPS approved mode (Full-FIPS mode) and all FIPS-related actions or procedures permitted on the module.

In order to operate the TippingPoint IPS securely, the user should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules and procedures.

4.1. Secure Operation

ENABLING APPROVED MODE OF OPERATION:

To operate in a FIPS-compliant manner, an IPS module must be placed in the approved mode of operation (called 'Full-FIPS' mode on the appliance) by using the following procedure:

- Ensure that the S660N and S1400N IPS models are updated to the 3.8.2 software release.
- After updating to the correct version of software, a Crypto-Officer (Super-user role on the appliance) must log in to the CLI over SSH and execute the following CLI commands:
  - ➢ conf t host fips-mode full
  - ➢ fips auth delete -add <superuser> -p *

The above mentioned CLI commands cause the IPS to do the following:

- Reboot
- Put the box into Full-FIPS mode
- Perform the FIPS power-up self tests
- Zeroize the keys
- Generate new keys
- Delete the existing user database and add the new default super-user specified in the "fips auth delete" command.
- Enable monitoring port traffic
- Enable the TLS and SSH servers
- Only use cryptographic algorithms allowed by FIPS
- Perform the conditional FIPS self-tests as needed

The above steps for the approved mode of operation ensure that the IPS meets the FIPS requirements for doing self tests, does not use the same keys and users in FIPS and non-FIPS modes, does not allow output during power-up self tests, uses only FIPS-approved cryptographic algorithms, etc. The IPS should now be operating in a FIPS compliant manner. If needed, the super-user can obtain a new TLS RSA key pair from TippingPoint and install it through LSM to replace the generated RSA key pair. Note that once the module is put into the FIPS-approved mode, it cannot be put back into a non-FIPS mode except by resetting the module to factory-defaults.

CHECKING FIPS MODE:

The current FIPS status can be shown with the "show fips" CLI command. In case of power-up or conditional self-test errors, the error can be seen in one or more of the following:

- Console port.
- System Logs, which can be seen using LSM GUI options or using "show log sys" CLI command.
- LSM GUI pop-up messages.

RUNNING POWER-UP SELF-TESTS:

To force the FIPS power-up self tests to be rerun, the user must power-cycle or reboot the appliance.

ZEROIZING KEYS:

To zeroize the keys, a super-user must log in to the CLI over SSH and execute the commands below. The zeroization will happen during the reboot.

- fips keys delete
- reboot -full

REGENERATING KEYS:

To regenerate the keys after they have been zeroized, a super-user must log in over the console port and execute the commands below. This can only be done over the console port since the SSH and TLS keys have been deleted. The generation will happen during the reboot.

- fips keys generate
- reboot -full

4.2. Security Rules

The security rules enforced by the TippingPoint IPS appliances include both the security rules that TippingPoint has imposed and the security rules that result from the security requirements of FIPS 140-2.

4.2.1 FIPS 140-2 Security Rules

The following are the security rules derived from the FIPS 140-2 requirements when in Full-FIPS mode:

- The TippingPoint IPS appliance supports identity-based operator authentication, access levels, and services as discussed in section 3.
- The TippingPoint IPS appliance supports CSPs and controls access to them as discussed in section 5.

- The TippingPoint IPS appliance has support for changing into Full-FIPS mode, zeroizing/generating keys, etc. See section 4.1 for more information.
- When in Full-FIPS mode, only cryptographic algorithms allowed by FIPS are used. See section 5.1 for the list of algorithms.
- The TippingPoint IPS module performs the following FIPS power-up self-tests on every power-up and reboot:
  - Firmware integrity test for all executable components using checksum. If a check fails, a message is displayed on the console and the IPS halts execution.
  - Known-answer self-tests for each cryptographic algorithm used by the module i.e. AES (encrypt/decrypt) KATs, Triple-DES (encrypt/decrypt) KATs, SHA (SHA-1/224/256/384/512) KATs, HMAC-SHA (SHA-1/224/256/384/512) KATs and RSA (sign/verify) KATs . If a test fails, a message is logged and the IPS reboots.
  - Known-answer self-test for the SP800-90A CTR_DRBG (DRBG Instantiate Function KAT, DRBG Generate Function KAT and DRBG Reseed Function KAT). If the test fails, a message is logged and the IPS reboots.
- The software performs the following FIPS conditional tests as needed:
  - Continuous random number generator tests for the approved SP800-90A CTR_DRBG and the non-approved RNG. If a test fails, a message is logged and the IPS reboots.
  - Software Load Test: When a user attempts to update the software/firmware, verify that the new software file was signed by the TippingPoint software/firmware load private key. If the signature check fails, the software update is aborted with no changes to the existing installed software. This validation is also done on software loads when FIPS mode is disabled. Because of this validation, the IPS meets the requirements for a limited operational environment.
  - Pair-wise consistency test after generating or installing new RSA keys. If the test fails, the new RSA key is ignored and will not be used.
- There is no data output from the data output interfaces of the IPS during the power-up self-tests.
- With the exception of feedback output of user passwords during their modification over the console port, no private or secret CSPs are ever output from the IPS. This option is disabled by policy as mentioned in the User and Crypto-Officer enforced rules below.
- All external entry of CSPs is encrypted with the exception of password entry over the console port.
- The user password is obscured during entry to the module.
- Non-FIPS service-access is not accessible in FIPS-approved mode. This service enabling is disallowed by the module while it is operating in Full-FIPS mode.
- The module does not support a FIPS bypass mode.

- In FIPS approved mode, the operator is not allowed to configure the password settings for less than 8 characters.
- Telnet and HTTP are disabled in Full-FIPS mode.
- The operator should use only FIPS approved cryptographic algorithms with SSH in Full FIPS mode.
- The operator should use only FIPS approved cryptographic algorithms with TLS 1.0 in Full FIPS mode.
- The IPS uses production-grade enclosure and components.

4.2.2 TippingPoint Security Rules

The following are the security rules that are enforced by TippingPoint when the IPS module is in Full-FIPS mode:

- TippingPoint always uses secure distribution means by making use of trusted third-party carriers such as UPS or FedEx for shipping the module to the authorized users.
- After receiving the module, it must be installed and initiated by a Crypto-Officer by following the procedure specified in the Crypto-Officer Guidance and in the documentation shipped with the module.
- No module operator has direct access to the internal storage on the IPS where the CSPs and installed software images are stored.
- If the module is reset to factory-defaults, it must be ensured that the module is using the firmware version specified in this document. If the module has been reset to an earlier version due to factory default action, it must be upgraded to this version.
- If remote authentication using a TippingPoint SMS Server is used, then only the SMS level 2 security setting should be used for establishing usernames and passwords on the SMS. This is required for meeting FIPS authentication strength requirements while authenticating to the IPS module. The level 2 setting on the SMS requires usernames to be a minimum of 6 characters and passwords to be a minimum of 8 characters, where 2 must be alphabetical, 1 must be numeric, and 1 must be non-alphanumeric.

4.3. Crypto-Officer Guidance

The following are the security rules that must be enforced or followed by the Crypto-Officer:

- The Crypto-Officer is responsible for a secure and successful installation, initialization and start-up of the module. The Crypto-Officer should follow the directions provided in the documentation guide shipped with the module. The guide details the procedures to do the following:
  1) Attach device to a rack

2) Connect the console port of the module to a computer and access the module’s terminal.
3) Connect network connection segments to the module.
4) Connect the power.
5) Check the LEDs.
6) Using the console port, follow the prompt in the setup wizard to establish the Crypto-Officer authentication information and to configure the management options of the module.
7) This completes the initial setup configuration.

- Only the console port should be used for module initialization. The LCD and Keypad should not be used for module initialization and setup since it allows the plaintext display of username and password on the LCD.
- All physical ports and logical interfaces of the module are allowed for use by the Crypto-Officer. Please refer to the ‘Ports and Interfaces’ section for details.
- Use the console port only in a secure, controlled environment since the traffic is in plain text. In general, use the CLI over SSH instead of over the console port unless the console port is the only option (e.g. to restore keys after zeroization).
- Add, delete, modify and manage all user accounts as required.
- Refer to Table 6 of this document for the services and their inputs and outputs which are allowed in this role.
- Follow the steps in the section 4.1 for enabling FIPS mode, generating/zeroizing keys, etc. to ensure the IPS operates in a FIPS-compliant manner.
- For CLI commands that take a password such as the password modification and new user addition CLI commands, use the option to be prompted for the password (with the use of a ‘*’ in the command) rather than entering the password as part of the command. This will prevent the password from being visible to the module operator.
- In the user settings, do not enable RADIUS or TACACS+ authentication support.
- If remote authentication using a TippingPoint SMS Server is used, then only the SMS level 2 security setting should be used for establishing usernames and passwords on the SMS. This is required for meeting FIPS authentication strength requirements while authenticating to the IPS module. The level 2 setting on the SMS requires usernames to be a minimum of 6 characters and passwords to be a minimum of 8 characters, where 2 must be alphabetical, 1 must be numeric, and 1 must be non-alphanumeric.
- Keep the IPS in a secure environment and do not attempt to open the enclosure.
- In the password security settings, do not disable account lockout for repeated login failures or change the lockout period to less than 1 minute. This will ensure that the FIPS password strength requirements are met.
- If desired, install a new TLS RSA key pair through the LSM GUI after obtaining it from TippingPoint’s TMC website. This must only be done using HTTPS.
- Follow all rules applicable to the Crypto-Officer role as specified in this Security Policy document.

4.4. User Guidance

The following are the security rules that must be enforced or followed by the User:

- All physical ports and logical interfaces of the module are allowed for use by the User role. Please refer to ‘Ports and Interfaces’ section for details.
- Use the console port only in a secure, controlled environment since the traffic is in plain text. In general, use the CLI over SSH instead of over the console port unless the console port is the only option (e.g. to restore keys after zeroization).
- For CLI commands that take a password such as the password modification CLI command, use the option to be prompted for the password (with the use of a ‘*’ in the command) rather than entering the password as part of the command. This will prevent the password from being visible to the module operator.
- If remote authentication using a TippingPoint SMS Server is used, then only the SMS level 2 security setting should be used for establishing usernames and passwords on the SMS. This is required for meeting FIPS authentication strength requirements while authenticating to the IPS module. The level 2 setting on the SMS requires usernames to be a minimum of 6 characters and passwords to be a minimum of 8 characters, where 2 must be alphabetical, 1 must be numeric, and 1 must be non-alphanumeric.
- Keep the IPS in a secure environment and do not attempt to open the enclosure.
- Refer to Table 6 of this document for the services and their inputs and outputs which are allowed in this role.
- Follow all rules applicable to the User role as specified in this Security Policy document.

4.5. Physical Security Rules

The TippingPoint IPS appliances satisfy the requirements for FIPS 140-2 Level 1 Physical Security. The IPS appliances use production-grade enclosures and components. The outer enclosure of the module is made of production-grade steel. The IPS module should be kept in a secure environment and no operator should attempt to open the enclosure. No other specific physical security mechanisms are required.

5. Security Relevant Data Items and Access Control

This section specifies the TippingPoint IPS Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the IPS.

5.1. Cryptographic Algorithms

When in the approved mode of operation (Full-FIPS mode), the IPS module uses the cryptographic algorithms in the table below.

Table 8: FIPS Mode Cryptographic Algorithms

Algorithm Type	Modes/Mod sizes/Options	Certificate #	FIPS-approved
Signature Algorithms			
RSA	2048 bit modulus (Sign/Verify, Key Gen)	1867	Yes
Symmetric Algorithms			
AES	128, 192, 256 bit (ECB, CBC)	3624	Yes
Triple-DES	3-key (ECB, CBC)	2019	Yes
Hashing Algorithms			
SHA	Byte-oriented. SHA-1,224,256,384,512	3042	Yes
HMAC-SHA	Byte-oriented. SHA-1,224,256,384,512 (Minimum key size = 112 bits)	2376	Yes
Random Number Generators			
DRBG	SP800-90A DRBG: Block Cipher (CTR) with AES-256	952	Yes
Non-approved RNG	Only used to seed the SP800-90A DRBG; permitted for use in FIPS Approved Mode.	N/A	No
Key Establishment/Transport Algorithms			
Diffie-Hellman Key Agreement (used with SSH)	2048-bit ; Provides 112 bits of security strength ; Allowed for use in FIPS Approved Mode ;	N/A	No
RSA Key Transport (used with TLS)	2048 bit ; Provides 112 bits of security strength ; Allowed for use in FIPS Approved Mode	N/A	No
CVL	SP800-135 KDFs (SSH, TLS)	644	Yes

Note:

- The KDF (key derivation function) used in each of SSH and TLS protocols was certified by CAVP with CVL Cert. #644.
- SSH and TLS protocols have not been reviewed or tested by the CMVP or CAVP. Please refer to IG D.11, bullet 2 for more information.

The module generates cryptographic keys whose strengths are modified by available entropy. The encryption strength for each of the following generated keys is at least 112 bits: AES key encrypting key, TLS RSA key pair, SSH RSA key pair, TLS pre-master secret, and SSH Diffie-Hellman private exponent.

The IPS supports the following non-FIPS approved cryptographic algorithms when not in Full-FIPS mode. These algorithms are not allowed in FIPS mode of operation.

Table 9: Non-FIPS Mode Cryptographic Algorithms

Algorithm Type/Name	FIPS-approved
Symmetric Algorithms	
Blowfish	No
RC2	No
RC4	No
DES	No
Hashing Algorithms	
MD5	No
HMAC-MD5	No

Please note that HMAC-MD5 and MD5 are allowed in FIPS mode strictly for TLS 1.0.

5.2. *Cryptographic Keys, CSPs, and SRDIs*

While operating in a FIPS-compliant manner, the TippingPoint IPS module contains the following security relevant data items:

Table 10: SRDI Information

Security Relevant Data Item	SRDI Description	Size	Generation/ Entry	Storage	Output	Zeroization
DRBG entropy input	Entropy input to SP 800-90A Block Cipher (CTR) DRBG function used to construct DRBG seed	256 bits	Not entered. Generated using a non-approved RNG	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
DRBG seed	Input to the DRBG that determines the internal	384 bits	Not entered. Generated using DRBG derivation	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.

	state of the SP800-90A Block Cipher (CTR) DRBG		function. Includes the entropy input from the entropy source			
DRBG key	DRBG key used for SP800-90A Block Cipher (CTR) DRBG	256 bits	Not entered. Internal value derived as part of DRBG operation.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
DRBG V	DRBG V parameter used for SP800-90A Block Cipher (CTR) DRBG	128 bits	Not entered. Internal value derived as part of DRBG operation.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
Software load test key	RSA public key used to verify software upgrade, uses SHA-256	2048 bits	Not generated. Entered encrypted with TLS session key during software package install	Persistent: Stored in plain text on internal storage.	No	It is a public key so no need to zeroize.
Password	User password	8-32 chars	Not generated. Entered by the user encrypted with session key (TLS or SSH) or in clear text (console port).	Persistent: Hashed using SHA256 and stored on internal storage.	No (The option of specifying the password as part of some CLI commands is disallowed by module policy – Section 4.2)	Stored in hashed form so no need to zeroize.
Key	AES	128	Not entered.	Persistent:	No	Zeroized

encrypting key	symmetric key used to encrypt all private keys stored on internal storage	bits	Generated using SP800-90A CTR_DRBG during key generation.	Stored in plaintext in physically erasable part of internal storage.		when going into Full-FIPS mode, on deleting fips keys, or on reset to factory defaults.
TLS RSA key pair	RSA public and private keys used for TLS, use SHA-256	2048 bits	Generated using SP800-90A CTR _DRBG during key generation. A super-user or admin user can install a new official key pair encrypted with the TLS session key.	Persistent: Encrypted with the key encrypting key and stored on internal storage.	Public key is output to its peer as part of TLS negotiation. Private key is never output.	Stored in encrypted form so no need to zeroize.
TLS Pre-Master Secret	Shared secret exchanged using RSA Key Transport and used to derive the Master Secret	48 bytes	May enter encrypted with the module's RSA public key when the module acts as a TLS Server. If the module acts as a TLS Client, it is generated using SP800-90A CTR _DRBG.	Ephemeral: Stored in RAM	May be output encrypted with the peer's RSA public key when the module acts as a TLS Client. It is never output if the module acts	Zeroized on reboot or power cycle.

					as a TLS Server.	
TLS master secret	Master Secret used to derive the encryption and MAC keys for both ends of an TLS session	48 bytes	Not entered. Computed as part of TLS negotiation according to TLS 1.0 standard using the pre-master secret and nonces.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
TLS encryption key	AES/Triple DES symmetric key for TLS encryption in one direction	AES: 128, 192, or 256 bits; Triple DES: 168 bits	Not entered. Derived from master secret as part of TLS negotiation.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
TLS integrity key	MAC key for integrity in one direction	160 bits	Not entered. Derived from master secret as part of TLS negotiation.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
SSH Diffie-Hellman Exchange Values	Public value and private exponent used for SSH DH Key Exchange	2048-bit	Module's private exponent is generated during SSH negotiation using SP800-90A CTR_DRBG. The public value is derived from the private exponent and the DH group. The peer's DH public value enters the module according to SSH Standard.	Ephemeral: Stored in RAM	Public value is output to its peer as part of SSH negotiation. Private exponent is never output.	Zeroized on reboot or power cycle.
SSH DH Shared Secret	The shared secret established using SSH	2048-bit	Not entered. Derived by the module during SSH negotiation	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.

	DH exchange according to the SSH Standard		using DH parameters.			
SSH RSA key pair	RSA key pair	2048 bits	Not entered. Generated using SP800-90A CTR_DRBG during key generation.	Persistent: Encrypted with the key encrypting key and stored on internal storage.	Public key is output to its peer as part of SSH negotiation. Private key is not output.	Stored in encrypted form so no need to zeroize.
SSH session encryption key	AES/Triple DES symmetric key for SSH encryption in one direction	AES: 128, 192, or 256 bits; Triple DES: 168 bits	Not entered. Derived during SSH negotiation.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
SSH integrity key	MAC key for integrity in one direction	160, 256, 384, or 512 bits	Not entered. Derived during SSH negotiation.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.

5.3. Access Control Policy

The IPS allows controlled access to the SRDIs contained within it. The following table defines the access that the IPS services have to the SRDIs (i.e. R=read, W=write, Z=zeroize, D=delete). If no access is listed, the service does not use that SRDI.

Table 11: Access Control Policy

Service	DRBG SRDIs	Software load test key	User passwords	Key encrypting key	TLS RSA key pair	TLS pre-master secret, master secret, encryption key, and integrity key	SSH RSA key pair	SSH DH exchange values, DH shared secret, session encryption key, and integrity key
Enable Full-FIPS mode	WZ		WD	RWZ	W	Z	W	RZ
View FIPS status						R		R
Configure own password			W			R		R
Configure any user’s password and access level			W			R		R
Configure password restrictions and account lockout settings						R		R
Zeroize keys	WZ			Z	D	Z	D	RZ
Generate new keys	WZ			RWZ	W	Z	W	RZ
Install new TLS RSA key pair				R	RW	R		
Reboot	WZ					RZ		RZ
Install new firmware/software	WZ	RW				RZ		Z
Do FIPS power-up self-tests								
Login to CLI			R	R			R	RW
Login to LSM			R	R	R	RW		
Configure non-FIPS related admin level settings						R		R
Configure non-FIPS related super-user level settings						R		R
View non-FIPS related configuration						R		R
View non-FIPS related status						R		R

Intrusion prevention functionality on the monitoring ports.								

6. Mitigation of Other Attacks

The cryptographic module does not claim to mitigate any other attacks in a FIPS-approved mode of operation.