HEWLETT-PACKARD TIPPINGPOINT

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

HP TippingPoint Intrusion Prevention System

Hardware Version: S6100N
Firmware Version: 3.2.1.1639

Document Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

HP 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 HP TippingPoint Intrusion Prevention System (IPS) model S6100N and firmware version 3.2.1.1639.

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 HP TippingPoint's 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 HP 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 HP TippingPoint Intrusion Prevention System is referred to as the *IPS*, *HP TippingPoint IPS*, the *module*, or the *device*.

1.1. Purpose

This document covers the secure operation of the HP TippingPoint Intrusion Prevention System 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 HP 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

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
NDRNG	Non-Deterministic RNG
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
SSL	Secure Sockets Layer
TDES	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 HP 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.

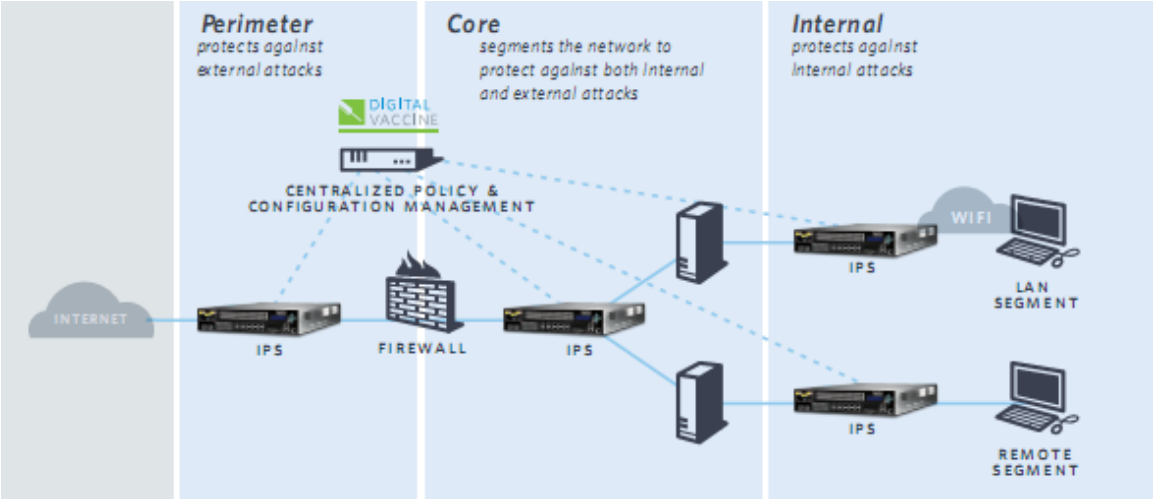

Figure 1: TippingPoint IPS Deployment in a Network

The HP 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.

HP 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 module), the HP TippingPoint IPS module meets the requirements applicable to Overall Level 1 of FIPS 140-2. The module claims higher levels in certain areas of security covered by the FIPS 140-2 Standard as listed below:

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

The physical configuration of the module is shown in the picture and table below:

Figure 2: TippingPoint S6100N IPS Module

The hardware specifications of the module are listed in the Table below:

Table 3: Hardware Specifications

IPS Model	Removable components	Dimension (H*W*D) (inches)	Monitoring Ports (excluded)	Management Interfaces	Inspection Through-put
S6100N	Fans, power supplies, external CF, SFP and XFP transceivers, and ZPHA module inserted in the ZPHA connector port	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 segment (2 ports) 10GbE XFP	1 10/100/1000 GbE Copper port, 1 RJ-45 Console port, 1 LCD and Keypad	8Gbps

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 outer hard metal enclosure of the module.

2.5 Components Excluded from FIPS 140-2 Security Requirements

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

1. Monitoring Ports

The module supports different types of monitoring ports i.e. Copper, SFP, and XFP. 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 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 and the ZPHA module:

The module has 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 and the ZPHA modules can never compromise the IPS module's security and are excluded from FIPS 140-2 security requirements.

2.6 Ports and Interfaces

The module 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 has 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.

USB PORT:
The module has 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 Button
	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. Roles

For each access method available, the module supports identity-based authentication, where each user has a Username and Password. 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 SSL, and can perform firmware upgrades to the module.	Crypto-Officer	Identity-based	Username and Password
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 module does not have support for a maintenance role. The module does not support bypass mode. 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).

3.2. 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 (disabled in Full FIPS mode)
- 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 SSL protection.
- Using the TippingPoint SMS Client GUI via SSL 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 SSL.

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

The module supports username-password authentication for all operators.

AUTHENTICATION STRENGTH:

When authenticating through the CLI, through LSM, or using the SMS client to the module in Full FIPS mode with remote authentication disabled, the module does the enforcement of user name and password restrictions. While in the 'Full' FIPS-mode, the module 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 the IPS module 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 module 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 module in Full FIPS mode with remote authentication disabled, the IPS module 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 module 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.

3.3. Module Services

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

Table 6: Module Services

Opera-tor	Admin-istrator	Super User	Service	Service Input	Service output	Notes
		Y	Enable/disable Full-FIPS mode	None	None	
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

Opera-tor	Admin-istrator	Super User	Service	Service Input	Service output	Notes
						below). Some keys (e.g. RNG seed and seed keys) 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	CLI prompt	

Opera-tor	Admin-istrator	Super User	Service	Service Input	Service output	Notes
				password, SSH parameters, input and data (when using SSH)	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 central management	Username and password, TLS parameters, input and data	System summary if successful and 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	None	None	Done automatically based on the

Opera-tor	Admin-istrator	Super User	Service	Service Input	Service output	Notes
			on the monitoring ports.			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 and generate ephemeral keys and CSPs	Reboot the module	None	None
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 Compact Flash eject switch	None	None
SNMP	Module automatically sends alert notifications if SNMP has been configured	None	Non-FIPS relevant data such as alerts, IPS network statistics. No key or CSP information is output by SNMP.

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 module 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, the 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 module is operating on the 3.2.1.1639 software release.
- After ensuring 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 and then enter a new password for the specified new Super-User, when prompted by the module.
  - 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 SSL 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 module 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 module 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 over TLS to replace the generated RSA key pair.

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 re-run, the operator must power-cycle or reboot the module.

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 SSL keys have been deleted. The generation will happen during the reboot.

- fips keys generate
- reboot -full

DISABLING FIPS MODE:
To disable Full-FIPS mode, a Super-User must log in to the CLI over SSH and execute the following commands:

- conf t host fips-mode disable
- fips auth delete -add <superuser> -p *

After this, the operator must enter a new password when prompted by the module. These CLI commands cause the module to perform the same steps as done when going into Full-FIPS mode except that the box is put into disabled FIPS mode, the FIPS self-tests are no longer performed, and the module may use cryptographic algorithms not allowed by FIPS.

4.2. Security Rules

The security rules enforced by the TippingPoint IPS module 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 module supports identity-based operator authentication, access levels, and services as discussed in section 3.
- The TippingPoint IPS module supports CSPs and controls access to them as discussed in section 5.
- The TippingPoint IPS module has support for changing into or out of 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, Triple-DES, SHA, HMAC-SHA and RSA. If a test fails, a message is logged and the IPS reboots.
    - Known-answer self-test for the ANSI X9.31 Random Number Generator. 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 ANSI X9.31 RNG and the NDRNG. If a test fails, a message is logged, the current output of the random number generator is ignored, and the software tries the random number generator again.
    - Firmware Load Test: When a user attempts to update the software/firmware, verify that the new firmware 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 firmware 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 module 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 operator 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.
- SSL 2.0 and SSL 3.0 support is disabled in Full-FIPS mode. Only TLS 1.0/SSL 3.1 is allowed.
- The module uses production-grade enclosure and components.

4.2.2 TippingPoint Security Rules

The following are the security rules that are enforced by TippingPoint:

- 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 operators.
- 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.
- The module allows for an external ZPHA module to be inserted in the ZPHA connector port on the module's body. If no ZPHA module is used, the ZPHA connector port must be covered with the blank bay faceplate provided with the module.
- 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/disabling 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.
- 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 (Sign/Verify)	1024, 2048 bit modulus	938	Yes
Symmetric Algorithms			
AES (ECB, CBC)	128, 192, 256 bit	1855	Yes
Triple-DES (ECB, CBC)	2-key and 3-key	1202	Yes
Hashing Algorithms			
SHA	Byte-oriented. SHA-1,224,256,384,512	1632	Yes
HMAC-SHA	Byte-oriented. SHA-1,224,256,384,512	1102	Yes
Random Number Generators			
RNG	ANSI X9.31: 3-key Triple-DES	973	Yes
NDRNG	Only used to seed the ANSI X9.31 RNG; Allowed for use in FIPS-Mode.	N/A	No
Key Establishment/Transport Algorithms			
Diffie-Hellman Key Agreement (used with SSH)	1024-bit ; Provides 80 bits of security strength ; Allowed for use in FIPS-Mode ;	N/A	No
RSA Key Transport (used with TLS)	2048 bit ; Provides 112 bits of security strength ; Allowed for use in FIPS-Mode	N/A	No

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

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
RNG seed	Seed for the ANSI X9.31 RNG	8 bytes	Not entered. Generated using NDRNG on every reboot	Ephemeral : Stored in RAM	No	Zeroized on reboot or power cycle.
RNG seed key	3-key Triple-DES seed key for the ANSI X9.31 RNG	3 keys of 8 bytes each	Not entered. Generated using NDRNG on every reboot	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 SSL 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 (SSL 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 encrypting key	AES symmetric key used to	128 bits	Not entered. Generated using ANSI	Persistent: Stored in plaintext in	No	Zeroized when going in or out of

Security Relevant Data Item	SRDI Description	Size	Generation/ Entry	Storage	Output	Zeroization
	encrypt all private keys stored on internal storage		X9.31 RNG during key generation.	physically erasable part of internal storage.		Full-FIPS mode, on deleting fips keys, or on reset to factory defaults.
TLS RSA key pair	RSA public and private keys used for SSL, use SHA-256	2048 bits	Generated using ANSI X9.31 RNG during key generation. A super-user or admin user can install a new official key pair encrypted with the SSL session key.	Persistent: Encrypted with the key encrypting key and stored on internal storage.	Public key is output to its peer as part of SSL 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 ANSI X9.31 RNG.	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 as a TLS Server.	Zeroized on reboot or power cycle.
TLS master secret	Master Secret used to derive the encryption and MAC keys for both ends of an SSL session	48 bytes	Not entered. Computed as part of SSL negotiation according to TLS 1.0 standard using the pre-master	Ephemeral : Stored in RAM	No	Zeroized on reboot or power cycle.

Security Relevant Data Item	SRDI Description	Size	Generation/ Entry	Storage	Output	Zeroization
			secret and nonces.			
TLS encryption key	AES/3DES symmetric key for SSL encryption in one direction	AES: 128, 192, or 256 bits; 3DES: 168 bits	Not entered. Derived from master secret as part of SSL 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 SSL 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	1024-bit	Module's private exponent is generated during SSH negotiation using ANSI X9.31 RNG. 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 DH exchange according to the SSH Standard	1024-bit	Not entered. Derived by the module during SSH negotiation using DH parameters.	Ephemeral: Stored in RAM	No	Zeroized on reboot or power cycle.
SSH RSA	RSA key	2048	Not entered.	Persistent:	Public key is	Stored in

Security Relevant Data Item	SRDI Description	Size	Generation/ Entry	Storage	Output	Zeroization
key pair	pair	bits	Generated using ANSI X9.31 RNG during key generation.	Encrypted with the key encrypting key and stored on internal storage.	output to its peer as part of SSH negotiation. Private key is not output.	encrypted form so no need to zeroize.
SSH session encryption key	AES/3DES symmetric key for SSH encryption in one direction	AES: 128, 192, or 256 bits; 3DES: 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	RNG seed and seed key	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/disable Full-FIPS mode	WZ		WD	RW Z	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			RW Z	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		

Service	RNG seed and seed key	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
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.