HotPort7000SP1.2

HotPort® 7000-Series Wireless Mesh Nodes: HotPort 7100 and HotPort 7200

Security Policy

Version: 1.2

Firetide, Inc.

Revision Date: June 21, 2013

CHANGE RECORD

Revision	***Date***	***Author***	***Description of Change***
0.1	09/01/09	Murali Repakula	Initial Release
0.2	10/22/09	Murali Repakula	Firetide updates
0.3	10/28/09	Murali Repakula	Firetide updates
0.4	11/05/09	Murali Repakula	Removing “root”, “ftusr” logins. Added AES128 & SHA1
0.5	11/09/09	Murali Repakula	Removing all references to SSH. Changed SSL to TLS
0.6	11/10/09	Murali Repakula	Adding HMAC keys
0.7	11/11/09	Paul Richards	Added 7100/7200 photos with tamper evidence labels
0.8	11/13/09	Murali Repakula	Added vendor rules, Firetide Build Public Key
1.0	12/10/09	Murali Repakula	Minor corrections per review comments
1.1	06/07/10	Murali Repakula	Excluding ‘mini PCI’ connector from FIPS 140-2 requirement Removing AAT from ‘unauthenticated’ service
1.2	06/21/13	Sudhir Hirudayaraj	Updated for firmware 7.9(F).0.0

Contents

Tables

Figures

1 Module Overview

The Firetide HotPort® 7000-Series Wireless Mesh Nodes: HotPort 7100 and HotPort 7200 (HW P/Ns HotPort 7100 and HotPort 7200, Version 1.0; FW Version 7.3(F).0.0 and 7.9(F).0.0) (hereafter referred to as the cryptographic module) are multi-chip standalone modules comprised of the HotPort 7100 model and the HotPort 7200 model.

The boundary of the cryptographic module is the outer enclosure.

The following non-security relevant components are excluded from the HotPort 7100 from the FIPS 140-2 requirements:

- Mini PCI connector
- Passive components, including various resistors and capacitors

Note: The antennas are not a part of the cryptographic boundary.

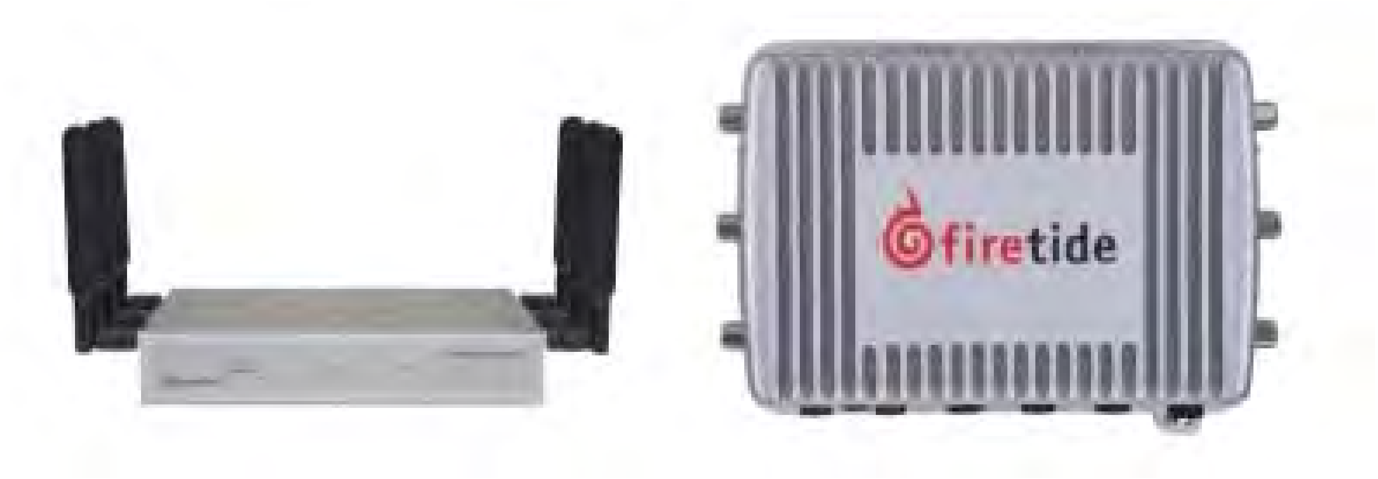


Figure 1 – Image of the Cryptographic Modules: HotPort 7100 (left) and HotPort 7200 (right)

Figure-2 (below) depicts a block diagram of the cryptographic module's hardware components, with the cryptographic boundary shown in red. The major blocks of the cryptographic module's hardware are:

- Memory: RAM, Flash and EEPROM
- CPU
- Network: Ethernet, Wireless
- Serial Port: Not accessible
- USB: Not used
- LEDs

This cryptographic module comes in two models, the first, model HotPort 7100, is meant for indoor operations and the second, model HotPort 7200, is for outdoor operations. The cryptographic boundary for both cryptographic modules is the outer enclosure. Upon power up, this cryptographic module comes up in FIPS operational mode upon verifying all the security functions of the cryptographic module.

This cryptographic module allows user management and control data to flow thorough ethernet and wireless interfaces. It is necessary to configure the end to end AES key prior to data flow to have the data encrypted. All unencrypted user data traffic entering through the ethernet is encrypted by CPU hardware by the user configured AES key. Only encrypted user data is sent or received over the wireless interface. The wireless interface is never used to terminate user traffic. Management traffic entering and leaving the ethernet and wireless interfaces are always encrypted by TLS. Control traffic may or may not be encrypted.

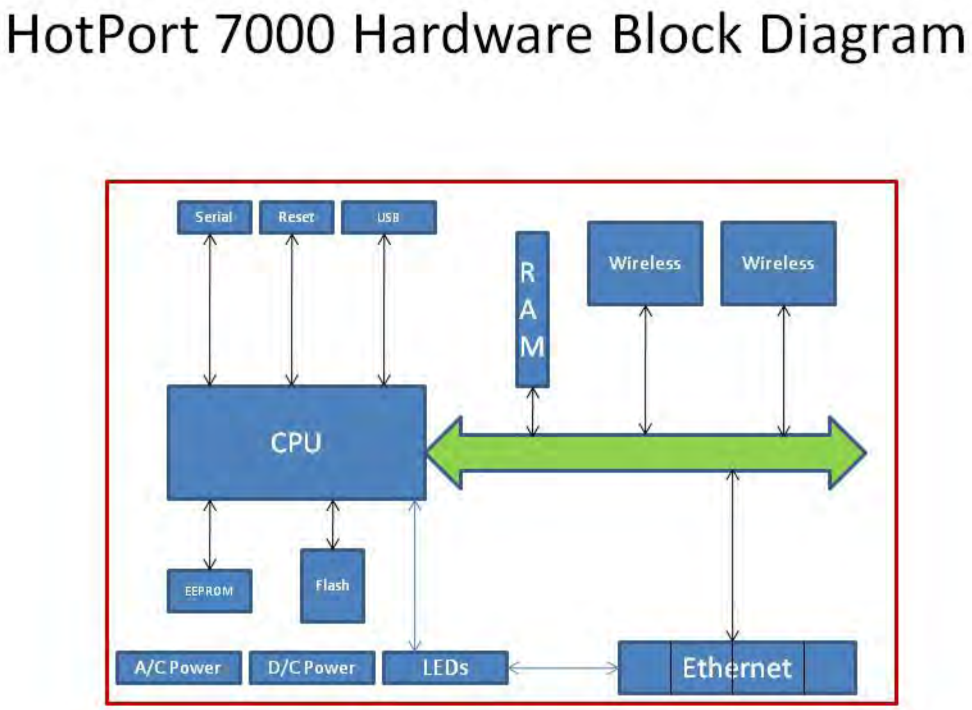


Figure 2 – HotPort® 7000 Wireless Mesh Nodes Block Diagram

1.1 Information flow among various hardware elements in HotPort 7000 Mesh nodes

The cryptographic module allows to be powered through A/C or D/C power.

EEPROM stores node information like the type of the node, serial number and network devices' (ethernet and wireless) mac addresses. CPU can read and write (program & reprogram) the information on the EEPROM.

Flash stores the loader, firmware and configuration of the node. CPU can read and write (program & reprogram) the storage on the flash.

USB port is currently disabled and doesn't participate in any activity on the nodes.

Serial port gives console access to the cryptographic module. Serial port is not accessible on FIPS nodes.

LEDs consist of status and ethernet activity LEDs. CPU controls status LEDs to show status about the Power, System, and wireless interface. Ethernet hardware updates ethernet activity LEDs.

RAM is used to load and run the firmware and store and forward data to and from ethernet and wireless interfaces. RAM can be accessed by the CPU for program execution and data storage and retrieval. RAM is accessed by ethernet to store packets received from the ethernet ports and for retrieval of packets that will be sent out on those ports. RAM is accessed by wireless interfaces to store packets received from the ethernet ports and for retrieval of packets that will be sent out on those interfaces. Management, control, and user data traffic enter and leave through ethernet and wireless interfaces. CPU performs required authentication, encryption, and decryption on the traffic as necessary.

Reset button allows for power cycle and factory default functions.

Cryptographic module services are described in Section 6 below.

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 – Cryptographic Module Security Level Specification

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

3 Modes of Operation

3.1 FIPS Approved Mode of Operation

The cryptographic module only provides a FIPS Approved mode of operation, comprising all services described in Section 6 below.

The cryptographic module will enter FIPS Approved mode following successful power up initialization. The cryptographic module will automatically indicate the FIPS Approved mode of operation by the 'status' LED turning solid green; FIPS mode can be confirmed by the solid green 'status' LED or through HotView (NMS) management software showing "FIPS" on the cryptographic module icon as shown in Figure 3.

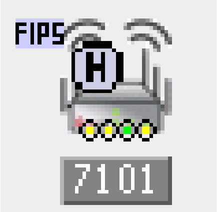


Figure 3 – HotView FIPS mode icon

This cryptographic module doesn't operate in Non-FIPS mode. Should FIPS mode fail, this cryptographic module sits in an error state shown by flashing 'status' LED. HotView (NMS) will not be able to login into the module and status would be represented as shown in Figure 4.

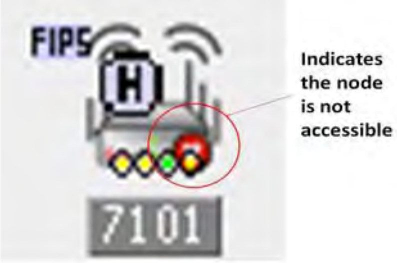


Figure 4 – HotView FIPS failure or Node down icon

3.2 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 2 – FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES: CBC, ECB; 128, 192, and 256 Used for encrypting & decrypting End to End Raw Data entering and leaving through ethernet interface. Referred to as 'End to End PSK'	1114
AES: CBC 128 Used by TLS for encrypting management traffic	1235
RSA: 1024 Used by TLS during connection establishment and to verify externally loaded software.	592
SHA-1 Used by TLS as the digest for management traffic encrypted with AES CBC 128	1133
SHA-512 Used by TLS along with RSA key pair during connection establishment	1133
HMAC-SHA-1 Used by TLS session for data integrity check	720
ANSI X9.31 RNG Used by TLS to get random used during session establishment	618

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 3 – non-FIPS Approved Algorithms Used in Current Module

FIPS Allowed Algorithm
AES (non-compliant)128, 192, and 256 for WPA-2 on wireless interfaces **The usage of this algorithm is not FIPS tested and has no FIPS validation**
RSA Encrypt/Decrypt (key wrapping; key establishment methodology provides 80 bits of encryption strength)
NDRNG (used to seed the Approved RNG)

4 Ports and Interfaces

The cryptographic module is a Multi-chip Standalone module with ports and interfaces as shown below.

Table 4 – HotPort® 7000 Wireless Mesh Nodes Pins and FIPS 140-2 Ports and Interfaces

Port	FIPS 140-2 Designation	Name and Description
RJ45	Data input, Data output, Status output, Control input, Power input/output	Ethernet data traffic, control traffic, direct management traffic, TLS management and POE power input for HotPort 7100 indoor and HotPort 7200 output for outdoor ports. HotPort 7100 module contains 4 RJ45 ports and HotPort 7200 module contains 3 RJ45 ports.
Wireless	Data input, Data output, Status output, Control input	Wireless transmission interface, via TLS connection, traffic exchanged with peer nodes.
Reset Button	Reset or factory default	Allows power cycle or factory default of the cryptographic module.
USB	Not Used	This interface is not enabled at this time.
LED	Status output	LED lights demonstrate ethernet transmit and receive, wireless peer availability status, node status, and provides cryptographic module status.
A/C 100/240V	Power input	A/C power. This is only present for HotPort 7200 module.
DC 12V	Power input	D/C power.

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module supports four (4) distinct roles; NMS Admin (referred to as Crypto-Officer), NMS Guest (referred to as User), CLI kepolo, and Peer. The cryptographic module enforces the separation of roles by using separate sessions per authentication. There is one session created per authentication and no change of role is allowed within the same session. The cryptographic module only allows one session for NMS access either as an 'admin' or as a 'guest' at a given time.

Table 5 – Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
NMS Admin (CO)	This role has access to all services offered by the cryptographic module.	Role based	Username and Password Role based identity
NMS Guest (User)	This role has limited read access to node configuration and status information	Role based	Username and Password Role based identity
CLI kepolo	This role has a limited read only access to services offered by the cryptographic module	Role based	Username and Password
Peer	Provides peer to peer (module to module) connection through TLS for management purposes	Identity based	Using Firetide node certificate RSA 1024 Keypair

Table 6 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password – 5 characters minimum.	Each character could be from a set of upper & lower case alphabets (26 each), numbers (10), other displayable characters (12+) which totaling 64+. The probability that a random attempt will success or a false acceptance will occur is 1/(64^5) which is 1/(2^30) which is less than 1/1,000,000. If the authentication takes 2 seconds per attempt, less than 30 chances are possible in a minute. The probability of successfully authenticating to the cryptographic module within one minute is 30 * 1/(64^5) which is (2^5) * 1/(2^30) which is less than 1/100,000.
RSA 1024	The probability that a random attempt will succeed or a false acceptance will

public key authentication	occur is approximately ½^80, which is less than 1/1,000,000. If the authentication takes 2 seconds per attempt less than 30 chances are possible in a minute. The probability of successfully authenticating to the cryptographic module within one minute is 30 * 1/(2^80) which is less than 1/1,000,000.

6 Access Control Policy

6.1 Roles and Services

The cryptographic module supports the following authenticated services:

Table 7 – Authenticated Services

Service	Description
Exchange Traffic	Control and Management Traffic is exchanged between nodes.
Read Status	Read status of the cryptographic module and interface statistics.
Read Configuration	The operator can view the cryptographic module configuration.
Change Configuration	The operator can modify any cryptographic module configuration.
Read End to End PSK (AES Key)	The operator can export End to End PSK key into a file over TLS session.
Change End to End PSK (AES Key)	The operator can program and change End to End PSK key over TLS session.
Openssl Services	This includes TLS initiation and authentication.
AAT (Antenna Alignment Tool).	Used to align the antennas for optimal reception.
Power on Self-Tests	Power on self-tests performed on demand.

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 8 – Unauthenticated Services

Service	Description
Perform Self-Tests	Power on self-tests performed on demand via power cycle or reset of the cryptographic module.
Read Status	LED status can be read without any authentication.

Table 9 – Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Read Configuration	X		X	
Change Configuration		X		X
Read End to End PSK	X		X	

Change End to End PSK		X		X
Read Status	X			X
Exchange Traffic	X	X	X	X
AAT (Antenna Alignment Tool).	X			X
Power on Self-Test	X			X
Openssl Services	X	X	X	X
Remote Services				

6.3 *Roles & Services*

Table 10 – Specification of Roles

Service -> Roles	**Read Configu-ration**	**Change Configu-ration**	**Read End to End PSK (AES Key)**	**Change End to End PSK (AES Key)**	**Read Status**	**Exchance Traffic**	**Power on Self-Test**	AAT (Antenna Alignment	**Openssl Services**
NMS Admin (CO) Uses TLS With RSA/SHA512	X	X	X	X	X	X	X	X	X
NMS Guest (User) Uses TLS with RSA/SHA512	X				X	X	X	X	X
CLI kepolo (kepolo)	X				X	X	X		
Peer						X			X

6.4 *Definition of Critical Security Parameters (CSPs)*

The cryptographic module contains the following CSPs:

Table 11 – Private Keys and CSPs

Key Name	**Type**	**Description**
End to End PSK	AES 128/192/256	Used for data encryption
Node Certificate Private	RSA 1024 Private key	Used during TLS connection establishment

NMS Admin Password	PIN minimum 5 ASCII	Used for authenticating NMS Admin role
NMS Guest Password	PIN minimum 5 ASCII	Used for authenticating NMS Guest role
CLI kepolo Password	PIN minimum 5 ASCII	Used for authenticating CLI read only user
TLS Confidentiality Keys	AES 128	Used for encryption of TLS traffic
HMAC Keys	HMAC 128	Used for data integrity checks in TLS

6.5 Definition of Public Keys

The cryptographic module contains the following public keys:

Table 12 – Public Keys

Key Name	Type	Description
Firetide CA Key	RSA 1024	Used to validate node certificate
Firetide Node Key	RSA1024	Used for management traffic encryption
Firetide Build Key	RSA 1024	Used to verify firmware load image

6.6 Definition of CSPs Modes of Access

Table 13 defines the relationship between access to CSPs and the different cryptographic module services. The modes of access shown in the table are defined as:

- **G** = Generate: The cryptographic module generates the CSP.
- **R** = Read: The cryptographic module reads the CSP. The read access is typically performed before the cryptographic module uses the CSP.
- **W** = Write: The cryptographic module writes the CSP. The write access is typically performed after a CSP is imported into the cryptographic module, or the cryptographic module generates a CSP, or the cryptographic module overwrites an existing CSP.
- **Z** = Zeroize: The cryptographic module zeroizes the CSP.

Table 13 – CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
NMS Admin, NMS Guest, CLI kepolo	Openssl Services	R R	Firetide CA RSA Public Key Firetide Node RSA Public Key
NMS Admin	Change Configuration	W W W W W R W Z Z Z R Z	NMS Admin password NMS Guest password CLI root password CLI ftusr password CLI kepolo Passwords End to End PSK End to End PSK End to End PSK Firetide CA RSA Public Key Firetide Node RSA Key Pair Firetide Build RSA Public Key Firetide Build RSA Public Key

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module does not contain a modifiable operational environment.

8 Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2 for a Level 2 cryptographic module.

8.1 Module Rules

1. The cryptographic module shall provide four distinct operator roles. These are NMS Admin, NMS Guest, Peer, and CLI kepolo.
2. The cryptographic module shall provide role-based or identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. The cryptographic module shall provide a separate session per user authentication.
5. The cryptographic module shall clear previous authentications upon the authenticated user leaving the session.
6. The cryptographic module shall not allow changes in role in any session.
7. When the cryptographic module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
8. The cryptographic module shall perform the following tests:

A. Power up Self-Tests

1. Cryptographic algorithm tests
   a. AES Encrypt and Decrypt Known Answer Test, for Cavium hardware
   b. AES 128 Encrypt and Decrypt Known Answer Test, for OpenSSL (TLS) crypto library
   c. RSA Sign/Verify Known Answer Test
   d. SHA-1 Know Answer Test
   e. SHA-512 Known Answer Test
   f. HMAC-SHA-1 Known Answer Test
   g. RNG Known Answer Test

2. Firmware Integrity Test – 32-bit CRC

B. Critical Functions Tests

1. Certificate Validity test

C. Conditional Self-Tests

1. RNG input test – done during every power up
2. ANSI X9.31 RNG Continuous Test – whenever a RNG value is requested
3. Firmware Signature Verification – 1024-bit RSA signature verification upon load

9. The operator shall be capable of commanding the cryptographic module to perform the power up self-test by re-cycling power or rebooting the cryptographic module.
10. Power up self-tests do not require any operator action.
11. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
12. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the cryptographic module.
13. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
14. The cryptographic module supports concurrent operators and maintains separation between them.
15. The cryptographic module does not support a maintenance interface or role.
16. The cryptographic module does not support manual key entry.
17. The cryptographic module does not have any external input/output devices used for entry/output of data.
18. The cryptographic module does not enter or output plaintext CSPs.
19. The cryptographic module does not output intermediate key values.
20. The cryptographic module does not support generating or regenerating node certificates.
21. The cryptographic module does not allow direct user access to the system through wireless interfaces.

8.2 Vendor Imposed Security Rules

This section documents the security rules required by the Vendor to maintain the cryptographic module.

1. CO should change the default ‘NMS Admin’ password before any data operations.
2. CO should set ‘End to End PSK’ before any data operations.
3. Enforce a strong password policy and change them on a regular basis.
4. Inspect the cryptographic module regularly for damage, intrusion, and tampering.
5. Ensure that only authorized personnel access the cryptographic module.
6. Use a trusted host for HotView NMS that manages the cryptographic module.
7. Upgrade the cryptographic module only with approved firmware. Note: To maintain validation, only validated firmware should be loaded. Loading non-validated firmware will invalidate the cryptographic modules validation.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip standalone cryptographic module is production quality containing standard passivation. Firetide HotPort 7100 and HotPort 7200 are housed in metal enclosures. Both enclosures are opaque within the visible spectrum and have been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

Models HotPort 7100 and HotPort 7200 require tamper evident labels to be applied. It is the responsibility of the Crypto-Officer to apply the labels on the Firetide equipment prior to deployment and field use. The labels are serialized. The Crypto-Officer should make a record of the Firetide serial number and the corresponding label serial numbers used. The application of the labels is described in Figures 5 – 10.

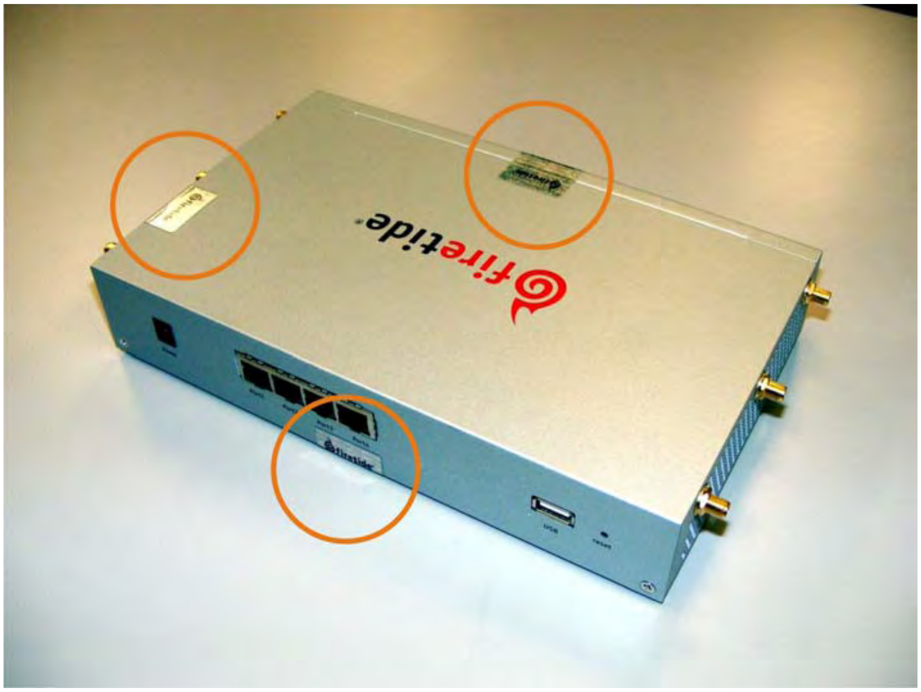
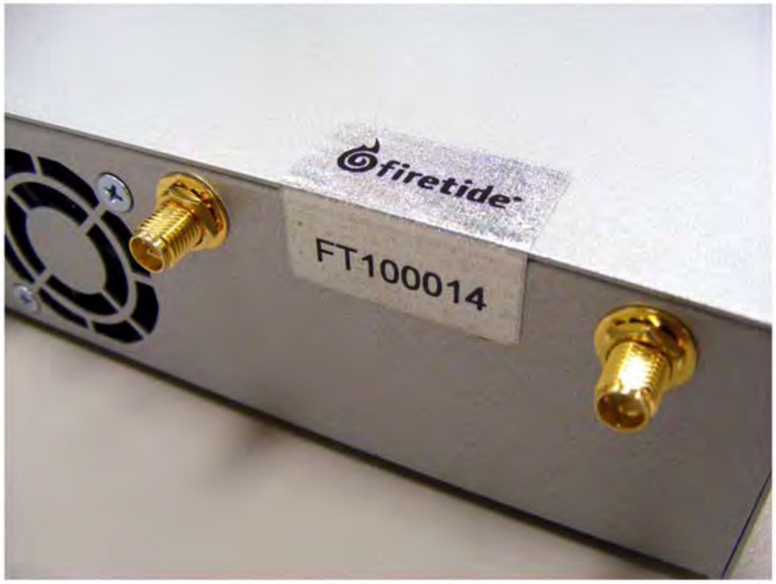


Figure 5 – Location of Tamper Evident Labels (3 Total) for the HotPort 7100

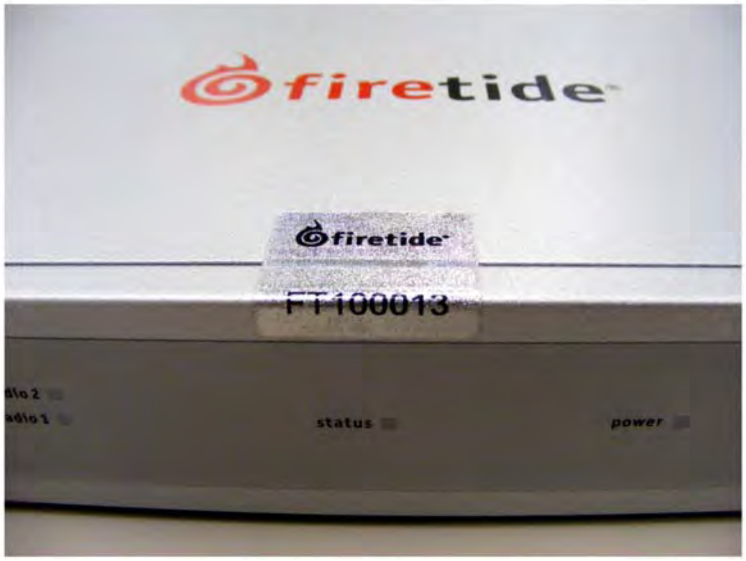
Prior to applying the labels, the areas at which the label will be applied must be cleaned using isopropyl alcohol (99%) and a lint-free cloth to assure optimum bonding of the label to the surface. It is recommended that the labels be applied at a temperature > 50 ^{o}F.

For the HotPort 7100, apply the three labels at the locations detailed in Figures 6 – 8.



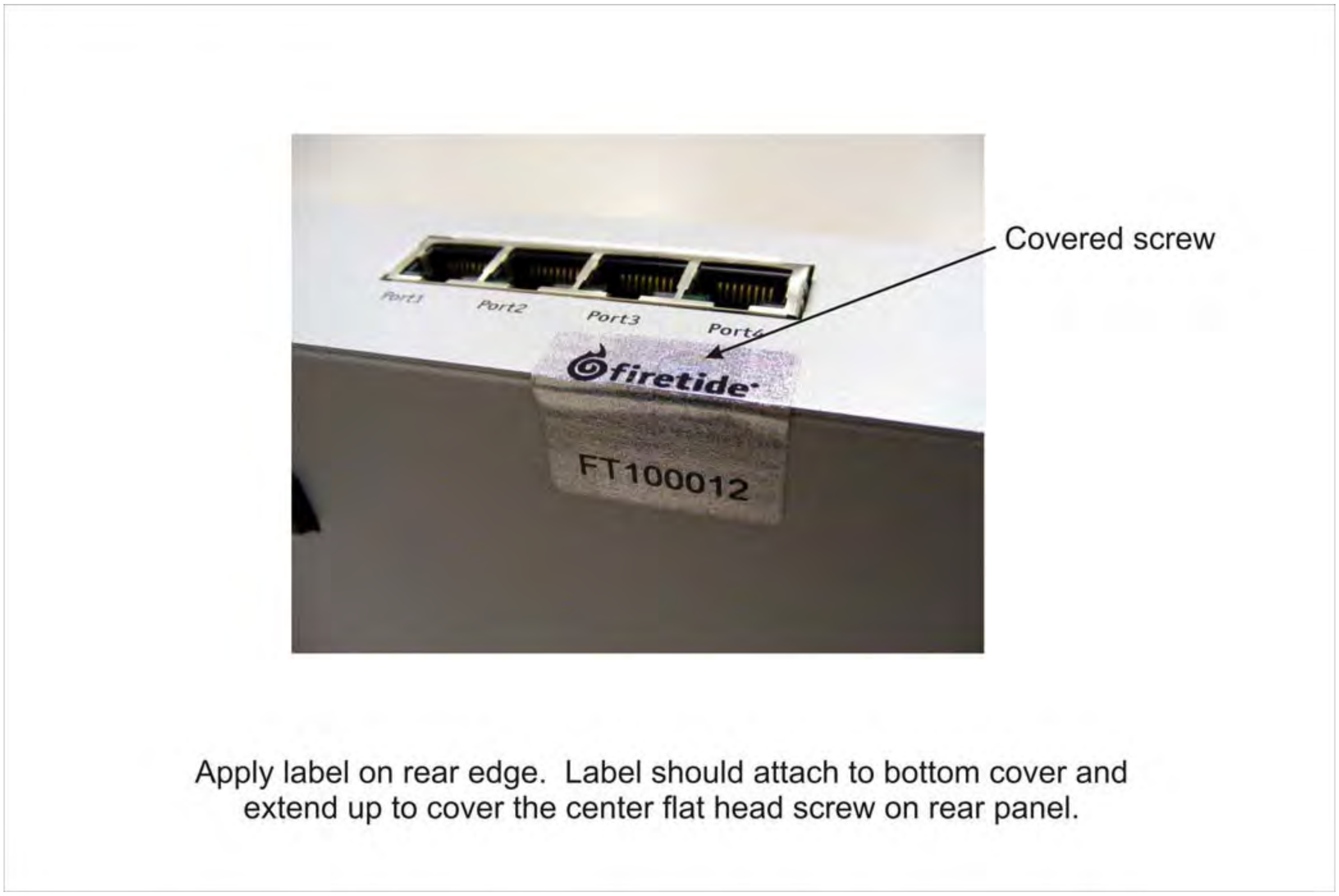
Apply label on right edge. Label should attach to top cover and extend down over seam and attach to side.

Figure 6 – Location of Right Side Tamper Evident Label on the HotPort 7100



Apply label on front edge. Label should attach to top cover and extend down over seam and attach to front panel.

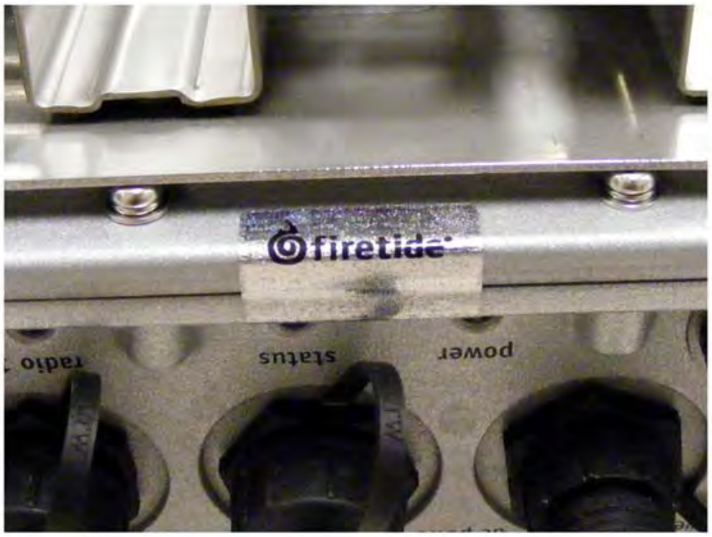
Figure 7 – Location of Front Side Tamper Evident Label on the HotPort 7100



Apply label on rear edge. Label should attach to bottom cover and extend up to cover the center flat head screw on rear panel.

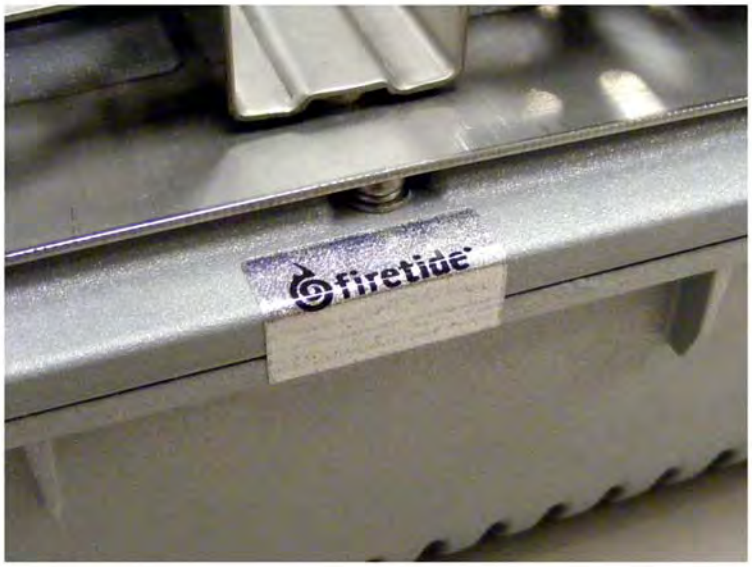
Figure 8 – Location of Rear Side Tamper Evident Label on the HotPort 7100

For the HotPort 7200, apply the two labels at the locations detailed in Figures 9 – 10.



Apply label to bottom edge of back cover. Label should wrap down to cover seam and attach to main enclsoure body.

Figure 9 – Location of Bottom Side Tamper Evident Label on the HotPort 7200



Apply label to top edge of back cover. Label should wrap down to cover seam and attach to main enclsoure body.

Figure 10 – Location of Top Side Tamper Evident Label on the HotPort 7200

The labels on each deployed unit should be periodically (every 3 months) inspected for evidence of tampering and for physical integrity. If the labels appear to have been tampered with, consult with customer support to determine if the cryptographic module should be zeroized and returned to the vendor for replacement.

10 Mitigation of Other Attacks Policy

The cryptographic module has not been designed to mitigate any attacks outside of the scope of FIPS 140-2.

11 References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

OpenSSL: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

12 Definitions and Acronyms

AES – Advanced Encryption Standard

CBC – Cipher Block Chaining

CO – Cryptographic Officer (Crypto-Officer)

CPU – Central Processing Unit

CSP – Critical Security Parameter

ECB – Electronic Codebook

EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

FIPS – Federal Information Processing Standards

FSM – Finite State Model

HMAC – Keyed-Hash Message Authentication Code

LED – Light-Emitting Diode

KAT – Known Answer Test

RNG – Random Number Generator

RSA – Rivest Shamir Adelman

SHA – Secure Hash Algorithm