GENERAL DYNAMICS
Mission Systems

Non-Proprietary Security Policy
for the FIPS 140-2 Level 2 Validated

Fortress Mesh Points

November 8, 2022 Version 1.13

This security policy of General Dynamics Mission Systems, for the FIPS 140-2 validated Fortress Mesh Points (FMP), defines general rules, regulations, and practices under which the FMP was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of products.

Hardware:

ES2440: High-Capacity Mesh Point

ES520 (V1 & V2): Deployable Mesh Point

ES820: Vehicle Mesh Point

Firmware: 5.4.7

REVISION HISTORY

Rev	Date	Description
1.0	May, 2016	Initial Draft
1.1	May, 2016	Various updates and edits
1.2	May, 2016	Various updates and edits
1.3	May, 2016	Formatting changes
1.4	May, 2016	Minor updates and edits
1.5	Sept, 2016	Several updates in response to lab review.
1.6	Feb, 2017	Updates to: Section 3.0 Identification and Authentication Policy Section 4.0 Cryptographic Keys and CSP. Section 6.0 Physical Security Policy Section 7.0 FIPS Mode. Various TLS and RSA updates.
1.7	April, 2017	Minor updates
1.8	June 15, 2020	Updates for 5.4.6
1.9	Jan 20, 2021	Additional updates for 5.4.6
1.10	March 5, 2021	Additional updates for 5.4.6
1.11	March 25, 2022	Updates for 5.4.7: SP800-56A-REV3 compliance. New ACVP certificate numbers for ‘Fortress Cryptographic SSL’ module.
1.12	Oct 25, 2022	Minor updates to table 10.
1.13	Nov 8, 2022	Minor updates to table 11.

Contents

LIST OF FIGURES AND TABLES

1.0 Introduction

Security policy for General Dynamics Mission Systems' Fortress Mesh Point (FMP) product line.

Throughout this Security Policy document, the security module will be referred to as 'FMP'.

The individual FIPS 140-2 security levels for the FMP are as follows:

Table 1: Security Level of Security Requirements

Security Requirement Security	Level
Cryptographic Module Specification	2
Cryptographic 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	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

2.0 Identification and Authentication Policy

The FMP supports up to 10 total users that can be defined. Each user is assigned a role as defined below.

2.1 Role-based Authentication

There are three Crypto Officer Roles. Please note that the configuration model supports assigning the roles below to users defined below. In this case, the role is a property of a defined user.

When creating a Crypto Officer, one of the roles described below must be selected along with a unique username and password. Although each operator has a unique username and password, since selecting a role is also required, therefore this system should be considered as having role-based authentication.

- Crypto Officer Roles
  - Log Viewer: account users can view only high-level system health indicators and only those log messages unrelated to configuration changes.
  - Maintenance[1]: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
  - Administrator: the main manager/administrator of the FMP.

- User Roles
  There are three User Roles.
  - MSP End User: This role will utilize another MSP secure controller to establish a secure connection over an untrusted network.
  - RSN End User: This role will utilize either a RSN (802.11i) secure client loaded on a workstation or a RSN (802.11i) secure controller like a VPN to establish a secure connection over an untrusted network.
  - IPsec/L2TP End User: This role will utilize either an IPsec/L2TP client loaded on a workstation or an IPsec/L2TP controller like a VPN to establish a secure connection.

2.2 Services

The following list summarizes the services that are provided by the FMP, refer to the User Guide for additional details.

- Encrypt/Decrypt (MSP | RSN | IPsec | SSH | TLS) PDU Services: use the encryption services of the FMP for passing of data.
- Show Status: observe status parameters of the FMP.
- View Log: view log messages.
- Write Configuration: change parameters in the FMP including changing the FIPS Mode, Bypass Setting, Zeroization and setting passwords;
- Read Configuration: read parameters in the FMP.
- Diagnostic: execute network diagnostic and self-tests services of the FMP.
- Upgrade: Upgrade the FMP with a new release of firmware.

[1] The Maintenance User is a CO and is not the same as a maintenance user as defined in FIPS 140-2.

2.3 Authentication and Authentication Data

All roles must be authenticated before they can use FMP services. This can be processed either internally by the FMP or externally using an EAP authentication server.

2.3.1 Authentication Methods

All roles must be authenticated if they use FMP services.

For Crypto-Officer authentication, a User Name and Password must be presented.

The FMP forces the Crypto-Officer to change the default password at first login.

The FMP will not accept new passwords that do not meet specified requirements.

A Crypto Officer can utilize three secure communication methods to access the FMP:

- Directly connected terminal
- Secure SSH (SSH-2.0-OpenSSH_5.8) connection
- Secure TLS connection (HTTPS)

A Crypto Officer can apply up to nine rules for administrative passwords that allow stronger passwords. These can be reviewed in the User Guide. FMPs having the same Access ID authenticate the MSP user. The RSN End User will use either a Shared Secret or will be authenticated by the use of an external EAP Server (i.e. RADIUS). The Authentication Data for each of these roles are shown in following table.

Table 2: Authentication Data

Operator	*Type of Authentication*	*Connect Using*	*Authentication Data*
Log Viewer	Password	Direct Connect Secure SSH HTTPS	The possible character space is 91([2]) characters and the password length is between 8 and 32 characters. (The default Log Viewer settings require a minimum of 15 characters).
Maintenance	Password	Direct Connect Secure SSH HTTPS	The possible character space is 91([2]) characters and the password length is between 8 and 32 characters. (The default Maintenance settings require a minimum of 15 characters).
Administrator	Password	Direct Connect Secure SSH HTTPS	The possible character space is 91([2]) characters and the password length is between 8 and 32 characters. (The default Administrator settings require a minimum of 15 characters).
MSP End User	Access ID	MSP	16-byte Access ID when in FIPS Mode. (In non-FIPS mode, users may select 8-bytes.
RSN End User	Secret	RSN	FIPS mode requires a 64-byte hexadecimal string (256 bits).
	ECDSA	RSN	Certificate base authentication supports ECDSA P-256 and ECDSA P-384.
IPsec/L2TP End User	Secret	IPsec/L2TP	FIPS mode requires a 32-256 byte hexadecimal string (128-1024 bits).
	ECDSA	IPsec/L2TP	Certificate base authentication supports ECDSA P-256 and ECDSA P-384.

[2]UI restricts the permitted characters to the all printable ASCII characters excluding double quote, single quote, and the apostrophe.

2.3.2 Authentication Server Methods

The Crypto Officer can also be authenticated by using an Authentication Server.

The Authentication Server can be:

1. The one built into the FMP.
2. On another FMP.
3. An external Authentication Server.

The service(s) available are determined by the FMP's configuration for authentication services as determined by the settings in Authentication Servers and/or Local Authentication.

To use an external server (RADIUS) for administrator authentication, it must be configured to use General Dynamic's Fortress Vendor-Specific Attributes (see User Guide for more information).

2.3.3 Authentication Strength

The probability of guessing the authentication data is shown in following table.

Mechanism	Role	Strength of Mechanism
Username & Password	Administrator Maintenance Log Viewer	The FMP requires that all variants of the Crypto Officer enter a valid username and password. There are 91 distinct characters allowed in the password, and the password may be between 8 and 32 characters. Assuming the low end of that range (8 chars), the probability of a successful random guess is 1 in 91^8 attempts. (or 1 in 4.70E+15) The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (4.70E+15/ (400*60)) or 1 in 1.96E+11. Note: The maximum number of login attempts can be set between 1 and 9 and lockout duration between 0 and 60 minutes.
MSP Shared Secret	MSP End User	The MSP shared secret is a 16 byte (128 bit) value. The probability of a random match is 1 in 2^128, or 3.40E+38. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (3.40E+38/ (400*60)) or 1 in 1.42E+34.
RSN Shared Secret	RSN End User	FIPS mode requires the RSN shared secret be entered as a 64-byte hexadecimal string (256 bits). The probability of a random match is 1 in 2^256, or 1.16E+77. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (1.16E+77/(400*60)) or 1 in 4.82E+72.
IPsec Shared Secret	IPsec/L2TP End User	FIPS mode requires the IPsec shared secret be entered as (32-256) byte hexadecimal string. Assuming the shortest length (32 hexadecimal string) that converts to 128-bits. The probability of a successful random guess is 1 in 2^128, or 3.40E+38. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (3.40E+38/ (400*60)) or 1 in 1.42E+34.
Certificate Based	RSN End User IPsec/L2TP End User	Certificate base authentication supports ECDSA P-256 and ECDSA P-384. For ECDSA P-256 the security bit strength is 128 bits, which means the probability of a random attempt succeeding is 1 in 2^128, or 3.40E+38. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (3.40E+38/ (400*60)) or 1 in 1.42E+34.

Table 3: Probability of guessing the authentication data

2.3.4 Administrative Accounts

The users are configured by adding administrative accounts to a Role. These are configured through the UI. For instance, the product can have multiple administrative accounts each having a unique Username and Password and each being assigned to a particular role (i.e., Log Viewer, Maintenance or Administrator). When a user is logged into the FMP he will have all the rights of the Role he has been assigned.

3.0 Cryptographic Keys and CSP

Keys and CSPs generated in non-FIPS mode cannot be used in FIPS mode, or vice versa. The FMP will require the admin to reboot the box after FIPS mode is enabled or disabled.

3.1 For MSP

The FMP contains a number of MSP cryptographic keys and CSPs, as shown in the following table. All keys are generated using FIPS approved algorithms and methods as defined in SP800-56A-REV3.

All keys are kept in RAM in plaintext, zeroized when the FMP reboots, and are never stored to disk.

Table 4: MSP Keys

Key	Key Type	Generation	Use	Implementation(s)
MSP Secret Key (MSK)	AES-CBC: 128, 192, or 256 bit.	Generated using the Access ID [3] as input into the SP 800-90A HMAC DRBG.	Used to encrypt static Diffie-Hellman public key requests and responses over the wire.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)
Static Private Key	Diffie-Hellman: 256 bits ECDH: 384 bits	Automatically generated using the SP 800-90A HMAC DRBG.	Along with received Diffie-Hellman Static Public Key from partner is used to generate the Static Secret Encryption Key	Fortress Cryptographic SSL
Static Public Key	Diffie-Hellman: 2048 bits ECDH: 384 bits	Automatically generated using Diffie-Hellman or ECDH.	Sent to communicating FMP in a packet is encrypted with MSK.	Fortress Cryptographic SSL
Static Secret Encryption Key	AES-CBC: 128, 192, or 256 bit.	Automatically generated using Diffie Hellman or ECDH.	Used to encrypt dynamic public key requests and responses over the wire.	Fortress Cryptographic SSL Fortress Cryptographic Implementation (FPGA)
Dynamic Private Key	Diffie-Hellman: 256 bits ECDH: 384 bits	Automatically generated using the SP 800-90A HMAC DRBG.	Along with received Dynamic Public Key from partner is used to generate the Dynamic Secret Encryption Key	Fortress Cryptographic SSL
Dynamic Public Key	Diffie-Hellman: 2048 bits ECDH: 384 bits	Automatically generated using Diffie-Hellman or ECDH.	Sent to communicating module in a packet encrypted with the Static Secret Encryption Key	Fortress Cryptographic SSL
Dynamic Secret Encryption Key (DKey)	AES-CBC: 128, 192, or 256 bit.	Automatically generated using Diffie Hellman or ECDH.	Used to encrypt all packets between two communicating FMPs	Fortress Cryptographic SSL Fortress Cryptographic Implementation (FPGA)
Static Group Key (SGK)	AES-CBC: 128, 192, or 256 bit.	Automatically generated using the SP 800-90A HMAC DRBG. [4]	Used to encrypt user-data frames until the unicast Dynamic Secret Encryption Key is computed.	Fortress Cryptographic SSL Fortress Cryptographic Implementation (FPGA)

[3] The Access ID is manually distributed by the Admin, refer to Section 3.5 'Additional Critical Security Parameters'.

[4] The static group key (SGK) is generated by using the Access ID (128 bits) merged with a MSP constant to seed an instance of an SP800-90A DRBG. Since the Access ID is 128 bits, this means that there is at most 128 bits of entropy in the static group key.

3.2 For RSN

An RSN or 802.11i wireless secure LAN can use either a PSK or an EAP generated master key.

If a PSK is used, each peer must configure the correct hex value. This PSK becomes the Master Key. If the EAP method is used, the Master Key is generated through the EAP process and it's correctly given to both the Client and FMP.

RSN are FIPS capable portions of the IEEE 802.11 specification for wireless LAN networks. The keys for RSN are shown in the following table.

AES-CCMP uses AES-CCM (allowed) in the 802.11i protocols (allowed). IEEE802.11i protocols are allowed in FIPS mode. Please see IG 7.2.

All keys are kept in RAM in plaintext, zeroized when the FMP reboots, and are never stored to disk.

Table 5: RSN Keys

Key	Key Type	Generation	Use	Implementation(s
Pairwise Master Key (PMK)	HMAC-SHA256	Using the key generation procedure as defined in the IEEE 802.11 specification. Input Material: WPA2-Personal mode: PSK [5] WPA2-Enterprise mode: uses key material generated during EAP authentication.	Authentication and to derive (PTK)	Fortress Cryptographic Implementation (Cryptlib)
Pairwise Transient Key (PTK)	For AES-CCM, 384 bit key comprised of three 128 bit keys: Data Encryption/Integrity key, EAPOL-Key Encryption key, and EAPOL-Key Integrity key.	PRF(PMK | AP nonce |STA nonce| AP MAC|STA MAC) PRF = RSN KDF (KBKDF #112)	Provides a set of keys used to protect link between end user station and FMP.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)
Group Master Key (GMK)	SP 800-90A DRBG Generated 256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification. Random number generated on the AP via SP 800-90A DRBG.	Used to derive (GTK).	Fortress Cryptographic Implementation (Cryptlib)
Group Transient Key (GTK)	For RSN, AES 256-bit key comprised of two 128 bit keys: Group Encryption key and Group Integrity key. For AES-CCM, 128 bit key comprised of Group Encryption/Integrity key.	PRF(GMK | APMac | GNonce) PRF = RSN KDF CAVP #112	Used to protect multicast and broadcast (group) messages sent from FMP to associated end user station. The AP sends the new GTK to each STA in the network using the PTK.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)

[5] WPA2-PSK: Plaintext (64 hexadecimal characters) or a (8-63) ASCII passphrase, compliant with manual distribution guidelines defined in FIPS 140-2 IG section 7.7.

3.3 For IPsec

An IPsec tunnel is created over an established AES encrypted RSN/802.11i wireless secure link. If the connection is over the external Ethernet port, then the IPsec tunnel is established over the current networking environment.

Please note, no parts of the IPsec protocol, other than the KDF, have been tested by the CAVP and CMVP.

The AES-GCM IV implementation follows the guidelines defined in RFC 4106 (sections 3.1, 4, & 8.1). The 96-bit IV consists of two parts, the leftmost 32-bits are randomly assigned per session key, and the rightmost value is a 64-bit TX counter. Each session key has a KB limit, which triggers a rekey, this prevents the counter from rolling over. This IV method is compliant with IG A.5 (Scenario #1) & Section 8.2.1 of the SP800-38D.

The modules uses RFC 7296 complaint with IKEv2 to establish the shared secret (SKEYSEED) from which the AES-GCM encryption keys are derived.

Only IPsec ECC keys are FIPS compliant, RSA keys are not permitted in FIPS mode. Refer to section '7.0 FIPS Mode' regarding FIPS required IPsec settings.

All keys are kept in RAM in plaintext, zeroized when the FMP reboots, and are never stored to disk.

Table 6: IPsec Keys

Key	Key Type	Generation	Use	Implementation(s)
DH Private Key	ECDH: 256/384 bits	Seed is automatically pulled from SP 800-90A DRBG	Used to calculate the DH Key	Fortress Cryptographic SSL
DH Public Key	ECDH: 256/384 bits	The DH Private Key is fed to the Diffie-Hellman function to automatically generate this key	Used for digital signature to authenticate the peer	Fortress Cryptographic SSL
ECDSA Private Key	ECDSA: 256/384 bits	Seed is automatically pulled from SP 800-90A DRBG	Used to calculate the ECDSA certificate Key	Fortress Cryptographic SSL
ECDSA Public Key	ECDSA: 256/384 bits	The ECDSA Private Key is fed to the ECDSA function to automatically generate this key	Used for digital signature to authenticate the peer	Fortress Cryptographic SSL
IKE-SKEYSEED	HMAC-SHA256 or HMAC-SHA384 Sz=(7*hash)	IKE-KDF (CAVP #937) As defined in SP800-135r1 Section 4.1 Internet Key Exchange	Generate IPsec SAs for ESP traffic	Fortress Cryptographic Implementation (Cryptlib) for hmac Fortress KAS Implementation for KDF Fortress Cryptographic Implementation (FPGA)
PSK	128bit – 1024bit	Manually distributed. [6]	Used for peer authentication, alternative to certificate authentication.	Fortress Cryptographic Implementation (Cryptlib)
Session Key	AES-GCM: 256 bits	Diffie-Hellman generated shared secret.	Used to encrypt/decrypt packets.	Fortress Cryptographic SSL

[6] IPsec PSK: Plaintext (32-256) hexadecimal characters or a (16-128) ASCII passphrase, compliant with manual distribution guidelines defined in FIPS 140-2 IG section 7.7.

3.4 For SSH and TLS

The SSH (SSH-2.0-OpenSSH_5.8) protocol uses the cryptographic algorithms of the OpenSSH protocol.

The TLS protocol is used to establish a secure connection from a management workstation running a standard internet browser (HTTPS). The GUI must only use ECC server keys to be FIPS complaint. Refer to section '7.0 FIPS Mode'.

The TLS 1.2 AES-GCM IV implementation is compliant with RFC 5288, IG A.5 (scenario 1) and SP800-38D (section 8.2.1). The 96-bit IV consists of two parts, the leftmost 32-bits are randomly assigned per session key, and the rightmost value is a 64-bit TX counter (per session key) increment per packet. The 64-bit counter would require several years([7]) of packets before producing a duplicate IV per session key. The implementation including the counter portion are entirely within the cryptographic boundary.

The TLS 1.2 module only supports the following cipher suites (SP800-52 Rev 1, Section 3.3.1):

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

All keys are kept in RAM in plaintext, zeroized when the FMP reboots, and are never stored to disk.

Please note, no parts of the SSH or TLS protocol, other than the KDF, have been tested by the CAVP and CMVP.

Table 7: SSH & TLS Crypto Keys

Key	Key Type	Generation	Use	Implementation(s
ECDSA Private Key SSH & TLS	ECDSA KEY 256 & 384 bits	Generated via openssl upon the 1st boot after a factory reset.	The private key is used to generate signatures.	Fortress Cryptographic -SSL
ECDSA Public Key SSH & TLS	ECDSA KEY 256 & 384 bits	Generated via openssl upon the 1st boot after a factory reset.	The public key is used to verify signatures.	Fortress Cryptographic -SSL
SSH Key Block	SSH KDF key block (SHA1, SHA256)	SSH-KDF (Cert # A2347) as defined in SP800-135r1 Section 5.2 (SSH Key Derivation Function)	The Key Block is the keying material that is generated for the AES encryption key. Encrypt Data Packets	Fortress Cryptographic -SSL.
TLS Key Block	TLS KDF Key block (SHA256,SHA384)	TLS-KDF ((Cert # A2347) as defined in SP 800-135r1 section 4.2.1	The Key Block is the keying material that is generated for the AES encryption key. Encrypt Data Packets	Fortress Cryptographic -SSL
TLS Pre Master Secret	Diffie-Hellman 256 & 384 bits	Generated via Openssl. The pre master secret is a shared secret generated by the negotiated key agreement scheme.	Input into the TLS KDF.	Fortress Cryptographic- SSL

[7] Generating 2million frames per sec over a 1gig network interface requires 292,471 years to max out the 64-bit frame counter.

3.5 Additional Critical Security Parameters

There are other critical security parameters present in the FMP as shown in the following table.

The non-volatile CSPs are stored encrypted and are zeroized when the FMP is restored to factory default; the volatile CSPs are stored in plaintext and are zeroized when the FMP is rebooted.

Table 8: Other Keys and Critical Security Parameters

CSP	Non-Volatile Storage	Type	Generation	Use	Implementation(s)
Access ID	Y	Seed	Manually distributed 32 hexadecimal plaintext digits (128 bits). [8] The administrator must use an approved DRBG when in FIPS Mode. Auto generation uses an instance of SP800-90A DRBG.	MSK, SGK & privD-H Group key component and used for authentication	Fortress Cryptographic Implementation (Cryptlib)
Log Viewer Password	Y	Password SHA256	8 to 32 Characters, entered by the Crypto Officer	To authenticate the Log View	Fortress Cryptographic Implementation (Cryptlib)
Maintenance Password	Y	Password SHA256	8 to 32 Characters, entered by the Crypto Officer	To authenticate the maintenance user	Fortress Cryptographic Implementation (Cryptlib)
Administrator Password	Y	Password SHA256	8 to 32 Characters, entered by the Crypto Officer	To authenticate the Administrator	Fortress Cryptographic Implementation (Cryptlib)
Firmware Upgrade Key	Y	RSA Public Key SHA256	Public RSA key (2048-bit) used to validate the signature of the firmware upgrade image that has been loaded from an external workstation.	Verify the signature that is attached to the upgrade package	Fortress Cryptographic SSL
Firmware Load Key	Y	RSA Public Key SHA256	Public RSA key (2048-bit) used to validate the signature of the firmware image that has been loaded from the internal flash drive at boot time.	Verify the signature that is attached to the firmware load package	Fortress Cryptographic SSL
HMAC DRBG entropy	N	Seed	Automatically Generated by ENT(P). Size=2*Configured Security Strength	Entropy used as input to SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)
HMAC DRBG V-Value	N	Counter	Automatically generated by DRBG	Internal V value used as part of SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)

[8] Access ID: Compliant with manual distribution guidelines defined in FIPS 140-2 IG section 7.7.

HMAC DRBG Key	N	Seed	Automatically generated by DRBG Size=2*Configured Security Strength	Key value used for the HMAC of the SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)
HMAC DRBG init_seed	N	Seed	Automatically generated by ENT(P) Size=2*Configured Security Strength	Initial seed value used in SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)
HMAC DRBG entropy	N	Seed	Automatically Generated by ENT(P) Size=2*Configured Security Strength	Entropy used as input to SP 800-90A HMAC DRBG	Fortress Cryptographic SSL
HMAC DRBG V-Value	N	Counter	Automatically generated by DRBG	Internal V value used as part of SP 800-90A HMAC DRBG	Fortress Cryptographic SSL
HMAC DRBG Key	N	Seed	Automatically generated by DRBG Size=2*Configured Security Strength	Key value used for the HMAC of the SP 800-90A HMAC DRBG	Fortress Cryptographic SSL
HMAC DRBG init_seed	N	Seed	Automatically generated by ENT(P) Size=2*Configured Security Strength	Initial seed value used in SP 800-90A HMAC DRBG	Fortress Cryptographic SSL

3.6 Known Answer and Conditional Tests

3.6.1 Known Answer Tests

This section describes the known answer tests run on the FMP.

The tests are organized by section against which they are run.

Table 9: Known Answer Tests

Known Answer Tests for CRYPTLIB	
Algorithm	**Modes/States/Key sizes/**
AES	**ECB(e/d; 128,192,256);** **CBC(e/d; 128,192,256)**
SHS	**SHA-1 (BYTE-only)** **SHA-256 (BYTE-only)** **SHA-384 (BYTE-only)** **SHA-512 (BYTE-only)**
HMAC	**HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS** **HMAC-SHA256 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA512 (Key Size Ranges Tested: KS=BS) SHS**
DRBG 800-90A	**Hash Based DRBG** **[HMAC_DRBG: SHA256, SHA512]**

Known Answer Tests for KAS	
KBKDF	**KDF SP800-108** **HMAC-SHA256, 16bit counter, After Fixed Data.**
IKE-KDF	**KDF SP800-135 (SHA-256 IKEV2)**

Known Answer Tests for FPGA **The FPGA algorithms are tested indirectly with packet KAT tests.** **(Encrypt;Decrypt) for each (MSP-Legacy, MSP-Suite B, ESP-Suite B, CCMP)**	
Algorithm	**Modes/States/Key sizes/**
AES	**CBC (e/d: 256)** **GCM (e/d: 256)** **CCM (e/d: 128)**
HMAC	**HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS**
Known Answer Tests for OPENSSL	

Algorithm	Modes/States/Key sizes/
AES	**ECB(e/d: 128)** **GCM(e/d: 256)**
SHS	**SHA-1 (BYTE-only)** **SHA-256 (BYTE-only)** **SHA-384 (BYTE-only)** **SHA-512 (BYTE-only)**
HMAC	**HMAC-SHA1 (Key Sizes : 160) SHS** **HMAC-SHA256 (Key Sizes : 160) SHS** **HMAC-SHA384 (Key Sizes : 160) SHS** **HMAC-SHA512 (Key Sizes : 160) SHS**
RSA	**ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-256**
ECDSA	**Sig(gen);Sig(ver);secp256r1 (P-256)** **Sig(gen);Sig(ver);secp384r1 (P-384)**
TLS-KDF	**KDF SP800-135 (SHA-256)**
SSH-KDF	**KDF SP800-135 (SHA-256)**
DH	**DH (Key sizes tested: 2048)**
ECDH	**ECDH-secp (Key Size Range: 384 bits)**
DSA	**Sig(gen);Sig(ver)** **(SHA384 Key:2048)**
DRBG 800-90A	**Hash Based DRBG:** **[SHA-1 , SHA-256 , SHA-384, SHA-512]**

3.6.2 Conditional Tests

This section describes the conditional tests run on the FMP.

Table 10 Conditional Tests

Tests	Condition
'Known Answer Tests' (Table 8)	**Power on self-test;** **FIPS mode change;** **Any security policy change**
Firmware Integrity Upgrade Test **RSA SIG(ver); 2048 , SHS: SHA-256**	**Firmware upgrade.**
Firmware Integrity Load Test **RSA SIG(ver); 2048 , SHS: SHA-256**	**Firmware image loaded at boot time.**
Pairwise Consistency Tests: **RSA(ALG[RSASSA-PKCS1_V1_5]** **SIG(gen); SIG(ver); 2048 , SHS: SHA-1** **DH(2048)** **ECDH(secp384)** **ECDSA([gen,ver], [secp256,secp384], [sha1])**	**Power on self-test;** **FIPS mode change;** **Any security policy change**
MSP Bypass Test	**Power on self-test;** **FIPS mode change;** **Change to the bypass mode** **Initialization of MSP peer**
CCMP Bypass Test	**Power on self-test;** **FIPS mode change;** **Change to the bypass mode** **Wireless interface initialization**
ESP Bypass Test	**Power on self-test;** **FIPS mode change;** **Change to the bypass mode**
Random Number Generation DRBG: **(Performs the HMAC_DRBG Health tests (Instantiate, Generate, and Reseed) as described in SP800-90A Section 11.3 Health Testing.**	**Power on self-test.** **Every generation of a random number**
ENT(P) – Startup Tests: **SHS; SHA-256**	**Power on self-test.**
ENT(P) – Continuous Tests: **APT (Adaptive Proportion Test)** **RCT (Repetition Count Test)**	**Power on self-test. ([9])** **Every sample retrieved from the noise source**

[9] The APT & RCT power on self-tests are performed using 4,096 samples.

3.7 Algorithm Certifications

This section describes the current list of certified algorithms and their certification numbers.

The listed the algorithm certificates may include other tested options/modes, only the modes/methods and key lengths/curves/moduli shown in this table are used by the module.

Table 11 Certifications

ALGO	Cert #	Crypto Implementation	Standard	Use	Operational Environment	Modes
AES	1519	Fortress Cryptographic Implementation V2.0	FIPS 197 SP 800-38A	Encrypt/Decrypt IPsec, WPA2, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	ECB (e/d: 128, 192, 256) CBC (e/d: 128, 192, 256)
	1520	Fortress Cryptographic Implementation FPGA V2.0	FIPS 197 SP 800-38A SP 800-38D	Encrypt/Decrypt IPsec, WPA2, MSP	Xilinx Spartan FPGA	CBC (e/d: 128, 192, 256) GCM (e/d: KS: 128 ,256) CCM (KS: 128)
	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS 197 SP 800-38A	Encrypt/Decrypt IPsec (IKE) WPA2 (establishment) SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	ECB (e/d: 128, 192 , 256) CBC (e/d: 128, 192, 256) CFB8 (e/d: 128, 192, 256) CFB128 (e/d: 128, 192, 256) OFB (e/d: 128, 192, 256)
	A2347	Fortress Cryptographic Implementation SSL V2.1.16	SP 800-38D	Encrypt/Decrypt TLS	RMI Alchemy MIPS Processor Broadcom XLS Processor	GCM (e/d:KS: 128, 192, 256)

CKG	Vendor Affirmed	Fortress Cryptographic Implementation SSL V2.1.16 Fortress Cryptographic Implementation V2.0 Fortress KAS Implementation V2.0	SP 800-133	Key Generation	RMI Alchemy MIPS Processor Broadcom XLS Processor	In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per SP800-133 using unmodified SP800-90A DRBG output. ([10])
ENT(P)	N/A	FPRBG Min-entropy of 1.0 per bit.	SP 800-90B	Entropy	RMI Alchemy MIPS Processor Broadcom XLS Processor	In accordance with FIPS 140-2 IG 7.18, the physical entropy source is complaint with SP 800-90B.
DRBG 800-90A	66	Fortress Cryptographic Implementation V2.0	SP 800-90A	Deterministic Rnd Bit Generation IPsec, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC_Based DBRG: SHA-256, SHA-512
DRBG 800-90A	A2347	Fortress Cryptographic Implementation SSL V2.1.16	SP 800-90A	Deterministic Rnd Bit Generation SSH WPA2 (establishment) IPsec (IKE) MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC_Based DBRG: SHA-1, SHA-256, SHA-384, SHA-512
DSA	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS186-4	IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	FIPS186-4 KeyPairGen: (2048, 224), (2048, 256), (3072, 256) SigGen/SigVer: (2048,224), (2048,256), (3072,256) ([11])
ECDSA	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS186-4	Signature Verify IPsec WPA2 (establishment) SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	SigVer: P-256, P-384

[10] The module directly uses the output from an approved DRBG to generate symmetric keys as well as the seeds to be used in FIPS 186-4 compliant asymmetric key generation.

[11] DSA: SigGen/SigVer only used in the self-tests.

ECDSA	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS186-4	Key Agreement IPsec WPA2 (establishment) SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	FIPS186-4: PKG: CURVES(P-256 P-384 ExtraRandomBits) PKV: CURVES(P-256 P-384)
ECDSA	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS186-4	Signature Generation IPsec (IKE) WPA2 (establishment)	RMI Alchemy MIPS Processor Broadcom XLS Processor	ECDSA SigGen: P-256, P-384 (SHA 256, 384)
HMAC	889	Fortress Cryptographic Implementation V2.0	FIPS198-1	Msg Authentication IPsec, WPA2, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512
HMAC	890	Fortress Cryptographic Implementation FPGA V2.0	FIPS198-1	Msg Authentication IPsec, WPA2, MSP	Xilinx Spartan FPGA	HMAC-SHA1 HMAC-SHA384
HMAC	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS198-1	Msg Authentication SSH WPA2 (establishment) IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512
IKE-KDF	CVL 937	Fortress KAS Implementation V2.0	SP800-135	Deriving Keys IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	IKEv1: AUTH(DSA , PSK)) 256 (SHA 1 , 256 , 384 , 512) 384 (SHA 1 , 256 , 384 , 512) 2048 (SHA 1 , 256 , 384 , 512) IKEv2: 256 (SHA 1 , 256 , 384 , 512) 384 (SHA 1 , 256 , 384 , 512) 2048 (SHA 1 , 256 , 384 , 512)
RSA	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS186-4	Signature Verify SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	ALG[RSASSA-PKCS1_V1_5] SIG (Ver) (2048 SHA(1, 256 , 384))

RSA	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS186-4	Signature Generation SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	ALG[ANSIX9.31] Sig(Gen): (2048 SHA(256 , 384)) ALG[RSASSA-PKCS1_V1_5] SIG (gen) (2048 SHA(256 , 384))
RSN-KDF (KBKDF)	112	Fortress KAS Implementation V2.0	SP800-108	Deriving Keys WPA2	RMI Alchemy MIPS Processor Broadcom XLS Processor	**CTR_Mode:** Length(Min32, Max2048) MACSupported([HMACSHA1] [HMACSHA256]) LocationCounter([AfterFixedData,BeforeFixedData]) rlength([8,16]))
SHS	A2346	Fortress Cryptographic Implementation Kernel V1.0	FIPS 180-4	Message Digest Entropy Module	RMI Alchemy MIPS Processor Broadcom XLS Processor	SHA-256 (BYTE-only)
SHS	1357	Fortress Cryptographic Implementation V2.0	FIPS 180-4	Message Digest IPsec, WPA2, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
SHS	1358	Fortress Cryptographic Implementation FPGA V2.0	FIPS 180-4	Message Digest IPsec, WPA2, MSP	Xilinx Spartan FPGA	SHA-1 (BYTE-only) SHA-384 (BYTE-only)
SHS	A2347	Fortress Cryptographic Implementation SSL V2.1.16	FIPS 180-4	Message Digest IPsec, WPA2, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only)SHA-512 (BYTE-only)
SSH-KDF	CVL A2347	Fortress Cryptographic Implementation SSL V2.1.16	SP800-135	Deriving Keys SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	SSH (SHA1, SHA-256)
TLS-KDF	CVL A2347	Fortress Cryptographic Implementation SSL V2.1.16	SP800-135	Deriving Keys TLS	RMI Alchemy MIPS Processor Broadcom XLS Processor	SSH (SHA256, SHA-384)
Safe Primes KeyGen/ Verify	A2347	Fortress Cryptographic Implementation SSL V2.1.16	SP800-56Ar3	Deriving Keys SSH, TLS, IPsec, WPA2, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	Safe Prime Groups: modp-2048, modp-3072, modp-4096, modp-6144, modp-8192

KAS-SSC	A2347	Fortress Cryptographic Implementation SSL V2.1.16	SP800-56Ar3	Key Agreement MSP (ECDH and DH)	RMI Alchemy MIPS Processor Broadcom XLS Processor	FFC: ffdhe2048, modp-2048 ECC: P-256, P-384 Key establishment methodology provides between 112 and 192 bits of encryption strength.
KAS	KAS-SSC Cert. #A2347 CVL Certs. #937 and #A2347	Fortress Cryptographic Implementation SSL V2.1.16 Fortress KAS Implementation V2.0	SP800-56Ar3 SP800-135	Key Agreement TLS, SSH, IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	See the referenced KAS-SSC and CVL Certs.

3.8 Non-approved Algorithms

Algorithm	Service	Allowed in FIPs mode
DSA KeyGen	SSH	No. Disabled while in FIPS mode.
MD5	NTP,RADIUS, TLS	Yes, this is allowed in the approved mode of operation when used as part of a key transport scheme where no security is proved by the algorithm.
RNG X9.31	MSP	No, provides backwards protocol compatibility when legacy mode is enabled and FIPS is disabled.
RSA KeyGen (FIPS 186-2)	IPsec, TLS, WPA2	No. Admin is not permitted to generate key pairs of type RSA. Refer to Section 7.0.
SNMP KDF	SNMP	No. Admin is not permitted to enable SNMP while in FIPS mode. SNMP provides read-only access to configuration and status information. Refer to Section 7.0
DH/ECDH	Legacy MSP	No, provides backwards protocol compatibility when legacy mode is enabled and FIPS is disabled.

The protocol SNMP shall not be used when operating in FIPS mode. In particular, none of the keys derived using the SNMP KDFs can be used in the Approved mode.

4.0 Access Control Policy

The same Crypto Officer may not be simultaneously logged in. However, the FMP supports concurrent login of different crypto-officer variants. An administrator and maintenance or other combination of crypto-officers may be logged in at the same time.

4.1 Roles and access to service

In general, a Crypto Officer is allowed to login and manage the FMP and end users can use cryptographic services. The following table shows a list of services and the roles which have access to them as shown in the following table.

Table 12: Roles each Service is authorized to perform

Role/Services	Encrypt/Decrypt [MSP | RSN | IPsec | SSH | TLS] PDU Services	Show Status	View Log	Write Configuration (including Bypass, Setting FIPS Mode, Setting Passwords, and Zeroization)	Read Configuration	Diagnostic (including self-tests)	Upgrade
Administrator	√	√	√	√	√	√	√
Maintenance		√	√		√	√	
Log Viewer			√				
MSP End User	√						
RSN End User	√						
IPsec/L2TP End User	√						

4.2 Roles and access to Keys or CSPs

The FMP doesn't allow access to the encryption keys; these are protected within the operating environment.

The following table lists the services that involve using cryptographic keys. (R=*Read* W=*Write* E=*Execute*)

Table 13: Roles who have Access to Keys or CSPs

Service	Access to Cryptographic Keys and CSPs	R	W	E
Encrypt/Decrypt [MSP | RSN | IPsec| SSH | TLS] PDU Services	MSP: MSP Secret Key, Static Group Key, Static Private Key, Static Public Key, Static Secret Encryption Key, Dynamic Private Key, Dynamic Public Key, Dynamic Secret Encryption Key RSN: PMK, PTK, GMK, GTK IPsec DH Private/Public Key, ECDSA Private/Public Keys, IKE-SKEYSEED, Session Key. PSK SSH: ECDSA Private Key, ECDSA Public Key, SSH Key Block TLS: ECDSA Private Key, ECDSA Public Key, TLS Key Block, TLS Pre Master Secret DRBG Cryptlib/SSL (Entropy, Key, init_seed, DRBG-V-Value)			√
Show Status	No access to crypto material			
Log View	No access to crypto material			
Write Configuration	Change own, Maintenance, and Log viewer password		√	
	Set Access ID *–random* (1) This set option will display the generated Access ID before it's confirmed and written to the database.	√ (1)	√	
	Set Access ID Set Bypass Set FIPS Mode Zeroization Set IEEE 802.11 PSK (RSN & IPsec) Digital Signature Generation and Verification Passwords		√	
Read Configuration	None of the configured crypto material can be read directly. Only an encrypted copy of these configured materials can be retrieved for the purpose of backing up the configuration.			
Diagnostics	No access to crypto material			
Firmware Boot and Load	Firmware Upgrade Key & Firmware Load Key			√

4.3 Zeroization

All keys and Critical Security Parameters are stored in a database and zeroized when:

- Restoring the factory defaults
- Manually replaced with new values.
- FMP is rebooted (for keys and CSPs stored in volatile memory)

Please refer to the appropriate User Guide to determine the actual zeroization process.

Table 14: Defaults and Zeroization

CSP	Reset value
Access ID	All Zeros
Administrator Password	Default Password
Log Viewer Password	Default Password
Maintenance Password	Default Password
PSK	All Zeros

4.4 Upgrades

4.4.1 Introduction

The FMP firmware can be upgraded in FIPS mode. The validated upgrade image is downloaded from a workstation via using the UI. The upgrade image is integrity checked and stored on the internal flash and booted. The previous image is kept stored on flash and can be selected as the boot image in case of problems with the upgrade image.

Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

4.4.2 Selecting Software Image

The FMP stores two, user-selectable copies (or images) of the FMP software on separate partitions of the internal flash memory. Please refer to the User Guide to determine how to select the image for execution.

5.0 Physical Security Policy

5.1 Hardware

The software executes one the following hardware platforms:

- ES520 Version 1
- ES520 Version 2
- ES820
- ES2440

5.2 Physical Boundary

All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements.

The FMP Firmware is installed by General Dynamics on a production-quality, FCC certified hardware device, which also define the FMP's physical boundary.

The physical boundary of the module is the perimeter of the module's casing, which is depicted as the borders of the box in the image below.

The cryptographic boundary does not include the IO related devices (serial, Ethernet, wireless adapters …) or the network stack code. The cryptographic boundary is concerned with the crypto algorithms, protocols, storage, and authentication. Refer to 'Figure 1 Physical Boundary vs Cryptographic Boundary'.

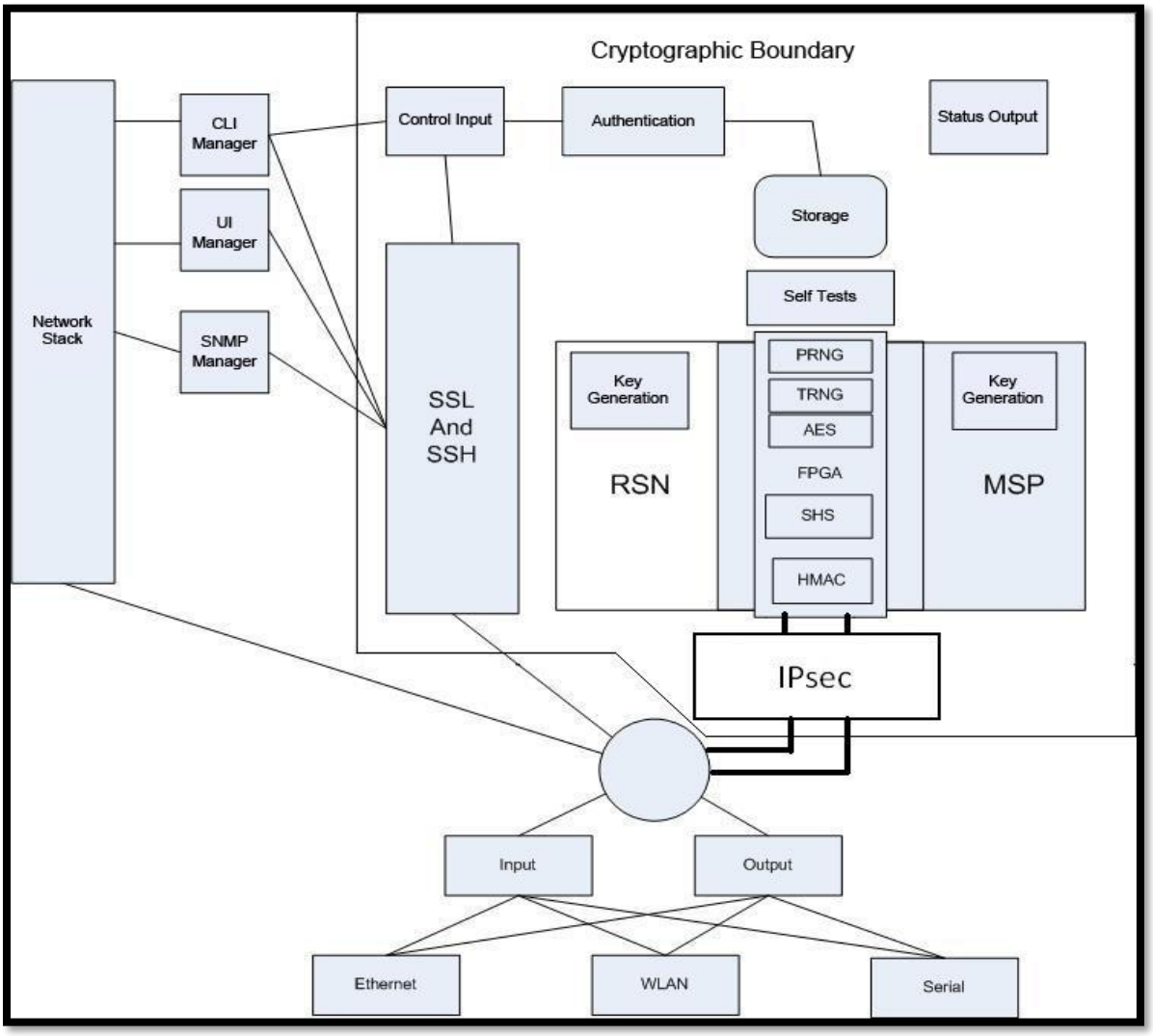

Figure 1 Physical Boundary vs Cryptographic Boundary

5.3 Tamper Evidence Application

These hardware platforms use Loctite 425 blue adhesive to cover screws for tamper evidence as shown in the following figures (2-7). The adhesive is applied during manufacturing. If the glue is removed or becomes damaged, it's recommended that the hardware be returned to General Dynamics to reapply.

5.4 Tamper Evidence Inspections

The following table details the recommended physical security activities that should be carried out by the Crypto Officer.

Table 15: Recommended Physical Security Activities

Physical Security Object	*Recommended Frequency of Inspection*	*Inspection Guidance*
Appropriate chassis screws covered with Loctite 425 blue epoxy coating.	Daily	Inspect screw heads for chipped epoxy material. If found, remove FMP from service.
Overall physical condition of the FMP	Daily	Inspect all cable connections and the FMP's overall condition. If any discrepancy found, correct and test the system for correct operation or remove FMP from service.

The host hardware platform server must be located in a controlled access area.

Tamper evidence is provided by the use of Loctite 425 blue epoxy material covering the chassis access screws.

Please note manufacturing may apply epoxy to additional screws, however the screws highlighted in the figures **must** be properly coated.

See the following figures (2-7) for the appropriate chassis screws.

Figure 2: ES2440 Tamper Evidence (2 screws)

Figure 3: ES820 Tamper Evidence (3 screws)

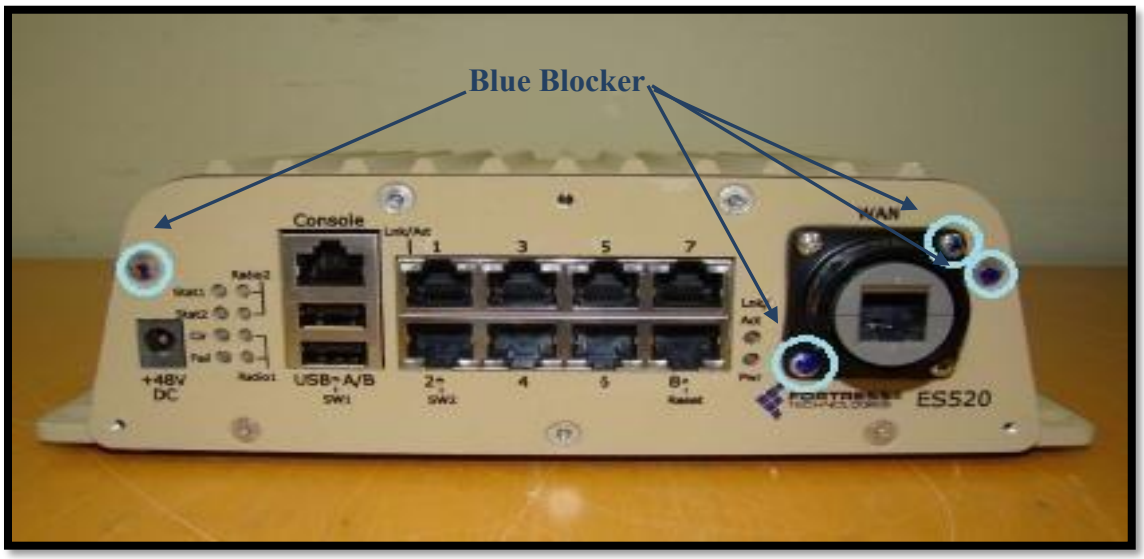

Figure 4: ES520 Version 1 (Front) Tamper Evidence (4 screws)

Figure 5 ES520 Version 1 (Rear) Tamper Evidence (4 screws)

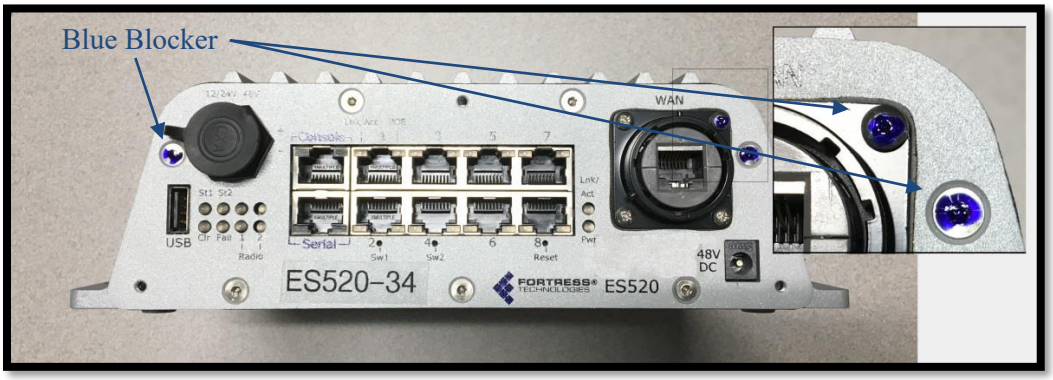

Figure 6 ES520 Version 2 (Front) Tamper Evidence (3 screws)

Figure 7 ES520 Version 2 (Rear) Tamper Evidence (4 screws)

Tamper Detection

If evidence of tampering is detected:

- Immediately power down the FMP.
- Disconnect the FMP from the network.
- Notify the appropriate administrators of a physical security breach.

6.0 Security Policy for Mitigation of Other Attacks Policy

No special mechanisms are built in the FMP; however, the cryptographic modules are designed to mitigate several specific attacks above the FIPS defined functions. Additional features that mitigate attacks are listed here:

- The MSP Dynamic Secret Encryption Key is changed at least once every 24 hours, with 4 hours being the factory default duration: Mitigates key discovery.
- In the MSP, the second Diffie-Hellman key exchange produces a dynamic common secret key in each of the FMPs by combining the other FMP's dynamic public key with the FMP's own dynamic private key: *Mitigates "man-in-the-middle" attacks*.
- In MSP, RSN and IPsec key exchanges after the first Diffie-Hellman exchange are encrypted: *Mitigates encryption key sniffing by hackers.*
- In MSP compression and encryption of header information inside of the frame, making it impossible to guess. MSP, RSN, or IPsec uses strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends*.
- In both MSP and RSN encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
- In MSP Multi-Factor Authentication: The FMP guards the network against illicit access with "multi-factor authentication", checking three levels of access credentials before allowing a connection. These are:
    - *Network authentication* requires a connecting device to use the correct shared identifier for the network
    - *Device authentication* requires a connecting device to be individually recognized on the network, through its unique device identifier.
    - *User authentication* requires the user of a connecting device to enter a recognized user name and password.

7.0 FIPS Mode

The following are the requirements for FIPS mode:

1. The FMP settings shall be initialized to factory default.
2. You must verify the FMP has the proper seals as described in section '6.0 Physical Security Policy'.
3. The FMP must be in FIPS Mode.
    - The operating mode can be determined by whether the CLI prompt displays a FIPS suffix; (e.g.: MP001-**FIPS**. The GUI Mode Indicator (Left Top of the GUI Screen) will show whether the FMP is in Normal or FIPS mode.
    - FIPS operating mode is the default mode of the FMP. Normal operating mode does not comply with FIPS. FIPS can be disabled or enabled through the management user interface (CLI or GUI) by the Administrator.
4. The following configuration guidelines are required for FIPS compliance. Failure to adhere to these guidelines will result in the module operating in a non-approved mode of operation:

Configuration Parameter	**CLI command**	**GUI**	
		Web Page	**Field**
Reset FMP to factory defaults	reset default	System Options	restore factory defaults
FIPS mode must be enabled; by default FIPS is enabled.	set fips on show fips	Security	operating mode
The SNMP agent must be disabled; by default SNMP is disabled.	set snmp –enable n show snmp	Not available on GUI	
The Access ID for a mesh network shall be generated using an approved DRBG	set accessid	Security	change access ID
The PSK shall be entered using hex values for RSN, the passphrase method shall not be used.	add bss –keytype hex update bss –keytype hex	Add BSS Edit BSS	preshared Key must be 'key'
WIFI Access Points must be configured to use WPA2-PSK or WPA2-enterprise mode. mode = [wpa2|wpa2psk]	add bss –1X11i <mode> update bss –1X11i <mode>	Add BSS Edit BSS	The 'Security Suite' selection must be 'wpa2psk' or 'wpa2'
The PSK shall be entered using hex values for IPsec, the passphrase method shall not be used.	set ipsec-psk -hex	IPsec Add Pre-shared Key	key type must be 'hex'
IPsec has to be configured as SuiteB128 or SuiteB256 only. V = [SuiteB256|SuiteB128]	set ipsec -crypto <v> show ipsec	IPsec Settings	suites

Configuration Parameter	CLI command	GUI	
IPsec sessions must be limited by KB usage. V >=1 and <=256,000,000	set ipsec –salifeKB <v> show ipsec	IPsec Settings	SA Lifetime
Only ECC type keypairs keys must be created. RSA2048 key types shall not be generated. V = [ec384|ec256]	generate keypair –type <v> generate csr –type <v> show keypair	Certificate	generate 'Key Pair and CSR'
Any configured external RADIUS network connection must be securely tunneled within an IPsec or MSP tunnel.	add auth update auth show auth	RADIUS	server list

8.0 Customer Security Policy Issues

General Dynamics Mission Systems expects that after the FMP's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the FMP(s) and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

9.0 Acronyms

Table 16: Acronyms

Acronym	Description
CKG	Cryptographic Key Generation
CSP	Critical Security Parameters
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic-curve Diffie-Hellman
FMP	Fortress Mesh Point: Fortress ES520 (Deployable Mesh Point), ES820 (Vehicle Mesh Point), and ES2440 (High-Capacity Infrastructure Mesh Point).
MSP	Mobile Security Protocol Fortress proprietary encryption protocol.
PDU	Protocol Data Unit. (a network frame)
PSK	Pre-Shared Key
RSN	Robust Secure Network Also known as WPA2.
UI	User Interface. Refers to the command line and the HTTPS browser management interfaces.