FIPS 140-2 Non-Proprietary Security Policy

McAfee Email Gateway EMG-5500-C and Email Gateway EMG-5000-C

Firmware Version 7.0.1

Document Version 1.5

August 11, 2014

Prepared For:

McAfee, Inc.

2821 Mission College Blvd

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the Email Gateway EMG-5500-C and Email Gateway EMG-5000-C.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSEC) jointly run the Cryptographic Module Validation Program (CMVP). The NIST National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates test reports for all cryptographic modules pursuing FIPS 140-2 validation. *Validation* is the term given to a cryptographic module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Email Gateway EMG-5500-C and Email Gateway EMG-5000-C from McAfee provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The McAfee Email Gateway EMG-5500-C and Email Gateway EMG-5000-C may also be referred to as the "module" in this document.

1.3 External Resources

The McAfee website (http://www.mcafee.com) contains information on the full line of products from McAfee, including a detailed overview of the Email Gateway EMG-5500-C and Email Gateway EMG-5000-C solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2014.htm) contains links to the FIPS 140-2 certificate and McAfee contact information.

1.4 Notices

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
MEG	McAfee Email Gateway
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
RSD	Remote Sensor Detection
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 McAfee Email Gateway EMG-5500-C and Email Gateway EMG-5000-C

2.1 Product Overview

McAfee Email Gateway integrates comprehensive inbound threat protection with outbound data loss prevention, advanced compliance, performance reporting, and simplified administration. By combining local network information with global reputation intelligence from McAfee Global Threat Intelligence, it provides the most complete protection available against inbound threats, spam and malware. Its sophisticated content scanning technologies, multiple encryption techniques, and granular, policy-based message handling prevent outbound data loss and simplify compliance. Administrators have the flexibility they need to create policies to fit their business, increasing the solutions performance. A single management console with enterprise-class logging and reporting capabilities simplifies administration and compliance workloads to significantly reduce costs.

More information on the McAfee Email Gateway solution can be found at http://www.mcafee.com/us/products/email-gateway.aspx.

2.2 Cryptographic Module Specification

The module is the McAfee Email Gateway EMG-5500-C and Email Gateway EMG-5000-C appliances running firmware version 7.0.1. Each appliance module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary is defined as the module case and all components within the case.

Once configured for FIPS mode of operation (see the Guidance and Secure Operation section), the module cannot be placed into a non-FIPS mode.

The physical boundary is pictured in the images below:

Module	Image
EMG-5500-C	
EMG-5000-C	

Figure 1 – Physical Boundary

Tested platforms and their processors are as follows:

EMG-5500-C	Intel 2x Xeon
EMG-5000-C	Intel Xeon

2.3 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Validation Level	**2**

Table 2 – Validation Level by DTR Section

The "Mitigation of Other Attacks" section is not relevant as the module does not implement any countermeasures towards special attacks.

2.4 Cryptographic Algorithms

2.4.1 Algorithm Implementation Certificates

The modules' cryptographic algorithm implementations[1] have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA 2048-bit	ANSI X9.31	1042	Sign operation
	RSA 1024, 1536, 2048-bit	ANSI X9.31	1042	Verify operation
	DSA 1024-bit	FIPS 186-2	639	Verify operation
Hashing	SHA-1, SHA-256	FIPS 180-2	1763	Hashing

[1] Please note that the standards for each algorithm are listed with the respective CAVP certificate.

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Keyed Hash	HMAC-SHA1	FIPS 198	1218	Message verification Message digest Module integrity
Symmetric Key	TDES (3-Key) CBC	FIPS 46-3	1299	Data encryption / decryption
	AES (CBC with 128bit keys)	FIPS 197	2013	Data encryption / decryption
Random Number Generation	X9.31	X9.31 (AES)	1055	Random Number Generation

Table 3 – FIPS-Approved Algorithm Certificates for OpenSSL Implementation ("Implementation A")

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA 2048, 3072, 4096-bit	FIPS 186-2	1080	Sign operation
	RSA 1024, 1536, 2048, 3072, 4096-bit	FIPS 186-2	1080	Verify operation
	DSA 1024-bit	FIPS 186-2	656	Verify operation
Hashing	SHA-1, 224, 256, 384, 512	FIPS 180-2	1829	Hashing
Keyed Hash	HMAC SHA-1, 224, 256, 384, 512	FIPS 198	1280	Message verification Message digest
Symmetric Key	TDES (3-Key) TECB, TCBC, TCFB	FIPS 46-3	1341	Data encryption / decryption
	AES (128,192,256) ECB, CBC and CFB128	FIPS 197	2106	Data encryption / decryption
Random Number Generation	X9.31	X9.31 (AES)	1081	Random Number Generation

Table 4 – FIPS-Approved Algorithm Certificates for OpenPGP Implementation ("Implementation B")

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA 2048-bit	X9.31, PKCS#1 V.1.5	1172	Sign / verify operations
	DSA 1024-bit	FIPS 186-3	711	Verify operation

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Hashing	SHA-1, SHA-256	FIPS 180-3	1963	Digital signature generation and verification (SHA-256) Verification of legacy data (SHA-1) User password hashing
Random Number Generation	FIPS 186-2 PRNG (Change Notice 1- with and without the mod q step)	FIPS 186-2	1134	Random Number Generation
Symmetric Key	AES 128-bit and 256-bit in CBC and ECB mode	FIPS 197	2281	Data encryption/ decryption
	TDES (3-key) CBC mode	FIPS 46-3	1429	Decryption of legacy data

Table 5 – FIPS-Approved Algorithm Certificates for McAfee Agent Implementation ("Implementation C")

Note the use of DSA/RSA 1024-bit and 1536-bit verify operations are for legacy use in accordance with FIPS 140-2 IG-G.14 and SP 800-131A transition tables. Use of SHA-1 hashing for digital signature verification of data is for legacy use and SHA-1 hashing for digital signature generation is disallowed in accordance with FIPS 140-2 IG-G.14 and SP 800-131A transition tables.

2.4.2 Non-Approved Algorithms

The module implements the following non-FIPS approved algorithms:

- Software-based random number generator
    - This RNG is used only as a seeding mechanism to the FIPS-approved PRNG.

- Diffie-Hellman
    - Key agreement; key establishment methodology provides 112-bits of encryption strength (allowed for use in FIPS mode of operation).
    - Key agreement; key establishment methodology provides less than 112-bits of encryption strength (non-compliant).

- RSA
    - Key wrapping; key establishment methodology provides 112-bits of encryption strength (allowed for use in FIPS mode of operation).

- Key wrapping; key establishment methodology provides less than 112-bits of encryption strength (non-compliant).

Implementation A	Implementation B	Implementation C
DES-CBC3-MD5	BLOWFISH	DES
DES-CBC-MD5	CAMELLIA128	MD2
DES-CBC-SHA	CAMELLIA192	MD5
DSA 1024-bit sign	CAMELLIA256	HMAC MD5
EDH-DSS-DES-CBC-SHA	CAST5	DES40
EDH-RSA-DES-CBC-SHA	DSA 1024-bit sign	RC2
EXP-DES-CBC-SHA	MD5	RC4
EXP-EDH-DSS-DES-CBC-SHA	RIPEMD160	RC5
EXP-EDH-RSA-DES-CBC-SHA	TWOFISH	ECAES
EXP-RC2-CBC-MD5	RSA 1024-bit sign	RSA PKCS#1 V.2.0 (SHA256 - OAEP)
EXP-RC4-MD5	RSA 1536-bit sign	
IDEA-CBC-MD5		
IDEA-CBC-SHA		
RC2-CBC-MD5		
RC4-MD5		
RC4-SHA		
RSA 1024-bit sign		
RSA 1536-bit sign		
DH 1024-bit		
DH 1536-bit		

Table 2-6 - Non-Approved Algorithms Per Implementation

The following algorithms are deprecated and will be disallowed according to timelines specified in NIST SP 800-131A:

- RSA (1024-bit and 1536-bit)
- DSA (1024-bit and 1536-bit)
- SHA-1
- HMAC-SHA1
- Diffie-Hellman
- RNGs specified in FIPS 186-2 and ANSI X9.31

2.5 Module Interfaces

The table below describes the main physical ports of each module:

Module	Physical Port
Email Gateway EMG-5500-C	• CD-ROM Drive (covered by bezel) • Gigabit Ethernet ports (x4) • LEDs – NIC 1, Power, System Status, ID, NIC 2, Hard Disk • Power interfaces (x2) • Power/Sleep button, Reset button, ID button, NMI button (covered by bezel) • Serial ports (two total, one covered by bezel) • Universal Serial Bus (USB) ports • Video Graphics Array (VGA) port
Email Gateway EMG-5000-C	• CD-ROM Drive (covered by bezel) • Gigabit Ethernet ports (x4) • LEDs – ID, System Status, Power • Power interfaces (x2) • Power/Sleep button, Reset button, ID button, NMI button (covered by bezel) • Serial port • Universal Serial Bus (USB) ports • Video Graphics Array (VGA) port

Table 7 – Module Ports and Interfaces

Each module provides a number of physical and logical interfaces to the device, and the physical ports provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Port
Data Input	GbE Ports
Data Output	GbE Ports
Control Input	GbE Ports LEDs Console Port On/Off Switch
Status Output	GbE Port LEDs Serial Port VGA Port
Power	Power interface

Table 8 – Logical Interface / Physical Port Mapping

The table below details the Email Gateway EMG-5500-C and Email Gateway EMG-5000-C LEDs and their color, condition, and description:

LED	Color	Condition	Description
Power/Sleep	Green	On	System On
		Blink	Sleep
	Off	Off	System Off
NIC1/NIC2 (5500-C only)	Green	On	NIC Link
		Blink	NIC Activity
System Status (on standby power)	Green	On	Running / Normal Operation
		Blink	Degraded
	Amber	On	Critical or Non-Recoverable Condition
		Blink	Non-Critical Condition
	Off	Off	POST / System Stop
Disk Activity (5500-C only)	Green	Random Blink	Disk Activity
	Off	Off	No Disk Activity

Table 9 – Module LEDs

2.6 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role, which are authorized via identity-based authentication. The module does not support a Maintenance role.

2.6.1 Operator Services and Descriptions

The services available to the Crypto Officer role are as follows:

Service and Description	Service Input	Service Output	Key/CSP Access
Configure Initializes the module for FIPS mode of operation	Configuration commands	Modified configuration file	None
Zeroize CSPs Clears CSPs from memory	Zeroize command or module reimage	Invalidated CSP	All CSPs

Table 10 – Crypto Officer Services and Descriptions

The services available to the User role are as follows:

Service and Description	Service Input	Service Output	Key/CSP Access

Service and Description	Service Input	Service Output	Key/CSP Access
Decrypt Decrypts a block of data Using AES or TDES	Key Encrypted byte stream	Byte stream	Symmetric Key: A Symmetric Key: B Symmetric Key: C
Encrypt Encrypts a block of data Using AES or TDES	Key Byte stream	Encrypted byte stream	Symmetric Key: A Symmetric Key: B Symmetric Key: C
Generate Keys Generates AES or TDES keys for encrypt / decrypt operations	Key Size	AES-Key TDES-Key	ANSI X9.31 PRNG seed: A ANSI X9.31 PRNG key: A ANSI X9.31 PRNG seed: B ANSI X9.31 PRNG key: B FIPS 186-2 PRNG Seed FIPS 186-2 PRNG Seed Key
Sign Signs a block with RSA or DSA	Data block to sign	RSA or DSA Signed data block	DH RSA Private Key DH DSA Private Key RSA Private Key: A DSA Private Key: A RSA Private Key: B DSA Private Key: B RSA Private Key: C DSA Private Key: C
Verify Verifies the signature of a RSA-signed or DSA-signed block	RSA or DSA Signed data block	Verification success/failure	DH RSA Public Key DH DSA Public Key RSA Public Key: A DSA Public Key: A RSA Public Key: B DSA Public Key: B RSA Public Key: C DSA Public Key: C
Key Generation Generate random number.	Entropy	Random number	ANSI X9.31 PRNG seed: A ANSI X9.31 PRNG key: A ANSI X9.31 PRNG seed: B ANSI X9.31 PRNG key: B FIPS 186-2 PRNG Seed FIPS 186-2 PRNG Seed Key
HMAC Hash-based Message Authentication Code	Key, data block	HMAC value	HMAC256 Key: A HMAC key: A HMAC key: B HMAC key: C

Table 11 – User Services and Descriptions

The module provides for the following unauthenticated services, which do not require authentication as they are not security relevant functions. These services do not affect the security of the module; these services do not create, disclose, or substitute cryptographic keys or CSPs, nor do they utilize any Approved security functions.

Service and Description	Service Input	Service Output	Key/CSP Access
Show Status Shows status of the module	None	Module status enabled/disabled	None
Initiate self-tests Restarting the module provides a way to run the self-tests on-demand	None	Console display of success/failure. Log entry of success/failure.	None

Table 12 – Unauthenticated Operator Services and Descriptions

2.6.2 Operator Authentication

2.6.2.1 Password-Based Authentication

In FIPS-approved mode of operation, the module is accessed via Graphical User Interface. Other than status functions available by viewing LEDs, the services described in Section 2.6.1 are available only to authenticated operators.

Passwords must be a minimum of 6 characters. The password can consist of alphanumeric values and special characters, {a-z},{A-Z},{0-9},{`~!@#$%^&*()_+={}[]\|;:'",./<>?], yielding 93 choices per character. The probability of a successful random attempt is $1/93^6$, which is less than 1/1,000,000.

Assuming a scripted attack of 60 attempts per minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/93^6$ which is less than 1/100,000.

The module will permit an operator to change identities provided the operator knows both the User password and the Crypto Officer password.

2.6.2.2 Certificate-Based Authentication

The module also supports authentication via digital certificates for remote sessions. The module supports a public key based authentication with 1024-bit, and 2048-bit RSA keys. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the

probability of a success with multiple consecutive attempts in a one-minute period is $60/2^{80}$ which is less than 1/100,000.

A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/2^{112}$ which is less than 1/100,000.

2.7 Physical Security

The module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. The module is completely contained within a production grade metal case with a hard plastic front bezel protected with a pick-resistant locking mechanism.

2.8 Operational Environment

Each module operates in a limited operational model and do not implement a General Purpose Operating System. The modules implement the following processors:

- EMG-5500-C: Intel Xeon X5660 2.80Ghz
- EMG-5000-C: Intel Xeon E5640 2.67Ghz

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
Firmware						
Crypto Officer Password	Alphanumeric passwords externally generated by a human user for authentication to the module.	Not generated by the module; defined by the human user of the module	On Disk / Plaintext	Never	Overwriting the passwords with new ones or module reimage	CO: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
User Password	Alphanumeric passwords externally generated by a human user for authentication to the module.	Not generated by the module; defined by the human user of the module	On Disk / Plaintext	Never	Overwriting the passwords with new ones or module reimage	User: RWD
Implementation A						
Symmetric Key: A	TDES or AES 128, AES 256	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Public Key: A	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Private Key: A	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Public Key: A	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Private Key: A	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
HMAC key: A	HMAC-SHA1 key	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
HMAC256 Key: A	HMAC-SHA256 key	Hardcoded at build time	RAM / Plaintext	None	Image wipe	CO: D USER: RWD
DH RSA Public Key	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH RSA Private Key	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH DSA Public Key	DSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	Yes	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH DSA Private Key	DSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
ANSI X9.31 PRNG seed: A	32-byte entropy	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
ANSI X9.31 PRNG key: A	AES 128	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
Implementation B						

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
Symmetric Key: B	TDES or AES 128, AES 192, AES 256	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Public Key: B	RSA 1024, 1536, 2048, 3072, 4096-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Private Key: B	RSA 1024, 1536 , 2048 , 3072 , 4096-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Public Key: B	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Private Key: B	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
HMAC key: B	HMAC SHA-1, 224, 256, 384, 512 Key	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
ANSI X9.31 PRNG seed: B	32-byte entropy	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
ANSI X9.31 PRNG key: B	AES 128	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
Implementation C						
Symmetric Key: C	TDES or AES 128, AES 256	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Public Key: C	RSA 2048-bit	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Private Key: C	RSA 2048-bit	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Private Key: C	1024-bit key	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
FIPS 186-2 PRNG Seed	Seed value for PRNG	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
FIPS 186-2 PRNG Seed Key	Seed key for PRNG	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

Table 13 – Module CSPs and Keys

Private, secret, or public keys are protected from unauthorized modification and substitution. The module ensures only authenticated operators have access to keys and functions that can generate keys. Unauthenticated operators do not have write access to modify, change, or delete private, secret, or public keys.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will enter an error state. When the module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions.

No keys or CSPs will be output when the module is in an error state. The module will halt and the process will terminate; as such, no data will be output via the data output interface. Additionally, the module does not support a bypass function, and the module does not allow plaintext cryptographic key components or other unprotected CSPs to be output on physical ports. No external software or firmware is allowed to be loaded in a FIPS mode of operation.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check via HMAC-SHA256
- RSA pairwise consistency key (signing and signature verification)
- DSA pairwise consistency key (signing and signature verification)
- TDES KAT (encryption and decryption on all modes and implementations)
- AES KAT (encryption and decryption on all modes, key sizes, and implementations)
- SHA-1, SHA-256, and SHA-512 KAT (on applicable implementations)
- HMAC-SHA1, HMAC-SHA256 and HMAC-SHA512 (on applicable implementations)
- PRNG KAT (on all implementations)

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

2.10.2 Conditional Self-Tests

Conditional self-tests are tests that run when certain conditions occur during operation of the module. If any of these tests fail, the module will enter an error state. The module can be restarted to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Pairwise consistency test for RSA implementations
- Pairwise consistency test for DSA implementations
- Continuous RNG test run on output of ANSI X9.31 PRNG implementations
- Continuous test on output of ANSI X9.31 PRNG seed mechanisms
- Continuous RNG test run on output of FIPS 186-2 PRNG implementations
- Continuous test on output of FIPS 186-2 PRNG seed mechanisms
- Continuous test to ensure seed and seed key are not the same values

The module does not perform a software load test because no additional software/firmware can be loaded in the module while operating in FIPS-approved mode.

2.11 EMI/EMC

Each module meets Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) Class A requirements as defined by 47 Code of Federal Regulations, Part15, Subpart B.

2.12 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Enabling FIPS Mode

To meet the cryptographic security requirements, certain restrictions on the installation and use of the module must be followed. The steps below will ensure that the module implements all required self-tests and uses only approved algorithms. Please note that once the module is in FIPS-approved mode, it cannot transition to a non-approved mode.

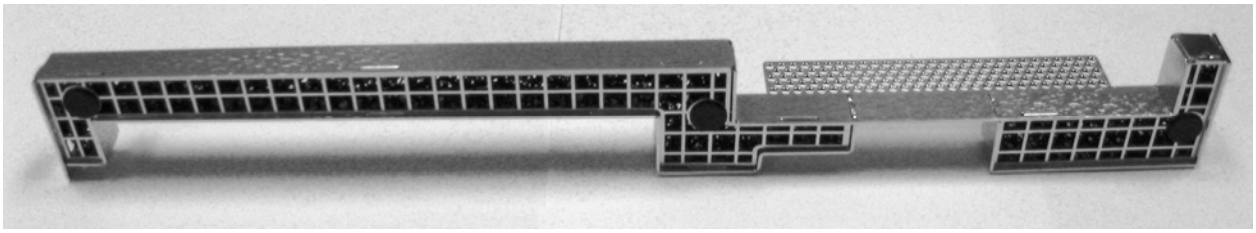
1. Verify that the firmware version of the module is Version 7.0.1. No other version can be loaded or used in FIPS mode of operation.
2. Select the FIPS mode option at installation.
3. Only 2048-bit asymmetric keys should be used where available.
4. The Crypto Officer password must be at least 6 characters in length.
5. Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.
6. Keys and CSPs shall be zeroized when transitioning to a FIPS mode from non-FIPS mode.
7. Ensure that the tamper evidence labels are applied as specified below. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.
8. Inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

The Email Gateway EMG-5500-C and Email Gateway EMG-5000-C meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation with respect to physical security.

3.1.2 FIPS Kit Installation

3.1.2.1 Installing the FIPS Kit on the model 5000

1. Attach the opacity baffle and affix tamper-evident seals to meet the physical tamper-evidence requirement for FIPS 140-2 Level 2 standards.
2. To obtain the FIPS kit, contact McAfee Sales to order SKU EWG-5000-FIPS-KIT.
3. Make sure the kit contains one opacity baffle and six tamper-evident seals. You will use five tamper-evident seals.



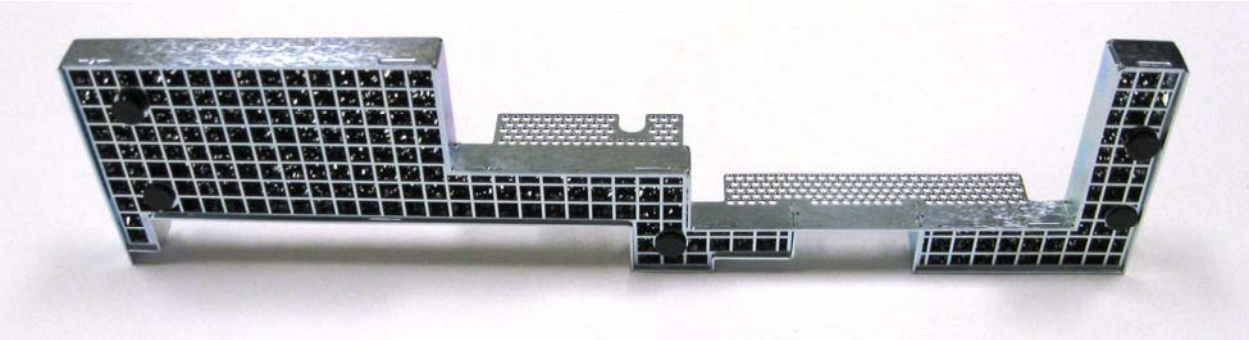
3.1.2.2 Install the opacity baffle

1. Locate the three fasteners on the baffle, and match them up with the openings on the rear of the appliance.
2. Push the fasteners into the openings. Once in place, the baffle is secure and cannot be remove without opening the top cover.

3.1.2.3 Installing the FIPS Kit on the model 5500

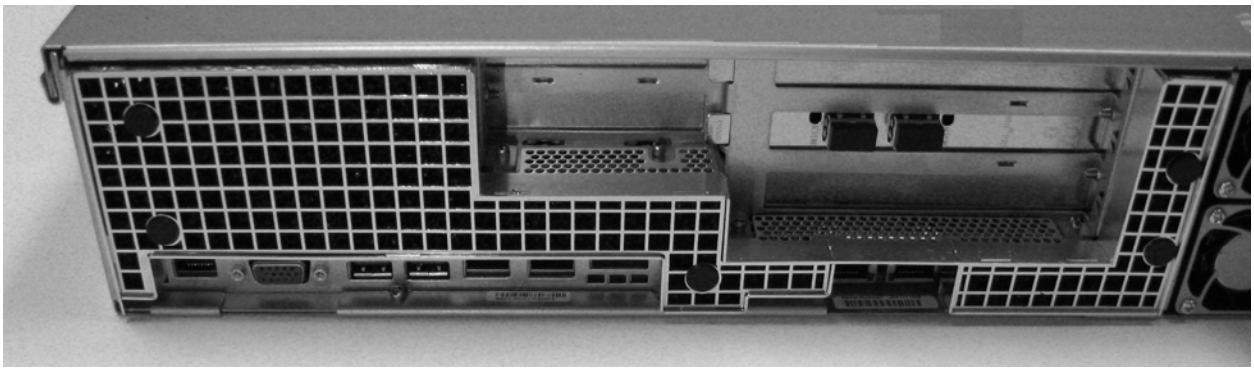
1. Attach the opacity baffle and affix tamper-evident seals to meet the physical tamper-evidence requirement for FIPS 140-2 Level 2 standards.
2. To obtain the FIPS kit, contact McAfee Sales to order SKU EWG-5500-FIPS-KIT.

3. Make sure the kit contains one opacity baffle and six tamper-evident seals. You will use five tamper-evident seals.



3.1.2.4 Install the opacity baffle

1. Locate the five fasteners on the baffle, and match them up with the openings on the rear of the appliance.
2. Push the fasteners into the openings. Once in place, the baffle is secure and cannot be remove without opening the top cover.



3.1.3 Applying Tamper-evident seals

The steps mentioned in the sections below should be performed by an authorized individual in order to apply the tamper-evident seals on the appliances.

After receiving the appliance, the Crypto Officer must apply the tamper-evident seals as described in the steps below. The model 5000 and 5500 platforms require 5 tamper-evident seals each. Two seals will be placed on the top of the chassis, one across the front bezel and one across the removable top panel. One seal will be placed on the bottom of the chassis, across the front bezel. The two power supplies located at the rear of the chassis will require one tamper-evident seal each. The seals must be placed on the appliance as indicated by red circles in the figures below. Follow these instructions to securely place the seals to the EMG-5000-C and EMG-5500-C modules:

1. To secure the front bezel, place a tamper-evident seal on the top such that it overlaps the front bezel and metal cover at the top of the chassis. (Figure 2 and Figure 4)

2. In order to secure the removable panel on the top of the appliance, apply a tamper-evident seal across the ridge. (Figure 5)

3. Continue to secure the front bezel by placing a tamper-evident seal on the bottom such that it overlaps the bottom portion of the bezel and the metal cover at the bottom of the chassis. (Figure 3 and Figure 6)

4. The tamper-evident seals have a 72 hour cure time. Please keep the extra tamper evident seal in a safe place.

Figure 2 – Model 5000 Seal Placement (Top)

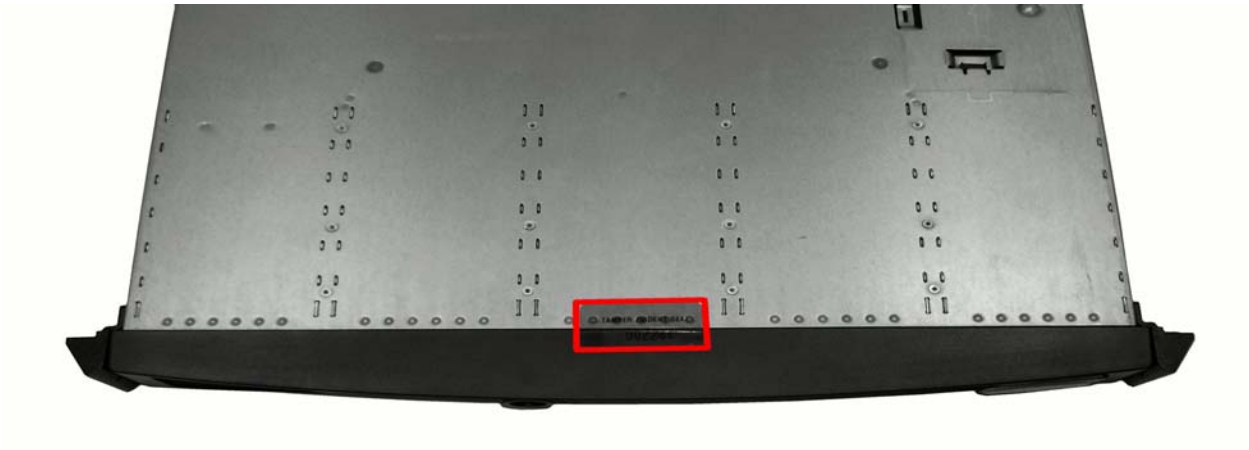


Figure 3 – Model 5000 Front Bezel Seal Placement (Bottom)

Figure 4 – Model 5500 Front Bezel Seal Placement (Top)

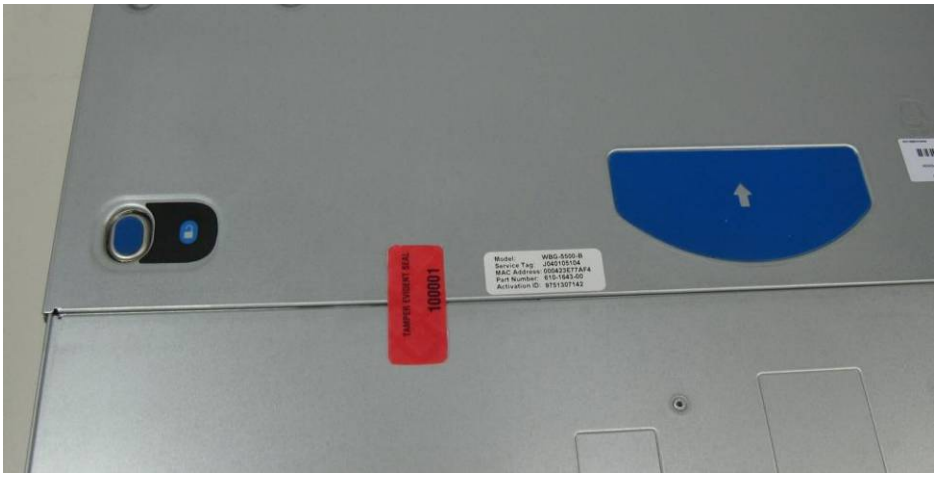


Figure 5 – Model 5500 Removable Panel Seal Placement

Figure 6 – Model 5500 Front Bezel Seal Placement (Bottom)

1. To secure the power supplies, place tamper-evident seals on the power supplies such that the seals are affixed to the top of the power supplies and chassis for model 5000 as indicated in Figure 7; and to the right side of the power supplies and chassis for model 5500 as indicated in Figure 8.

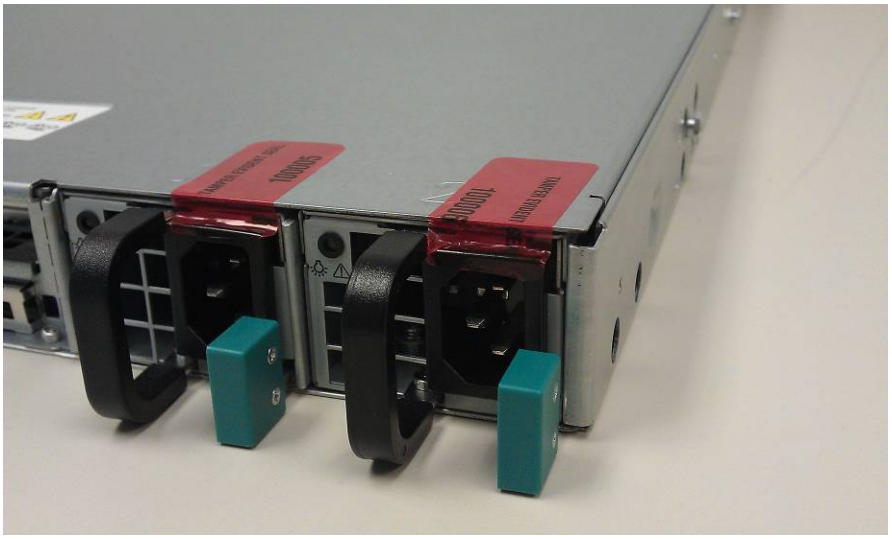


Figure 7 – Model 5000 Power Supply Seal Placement

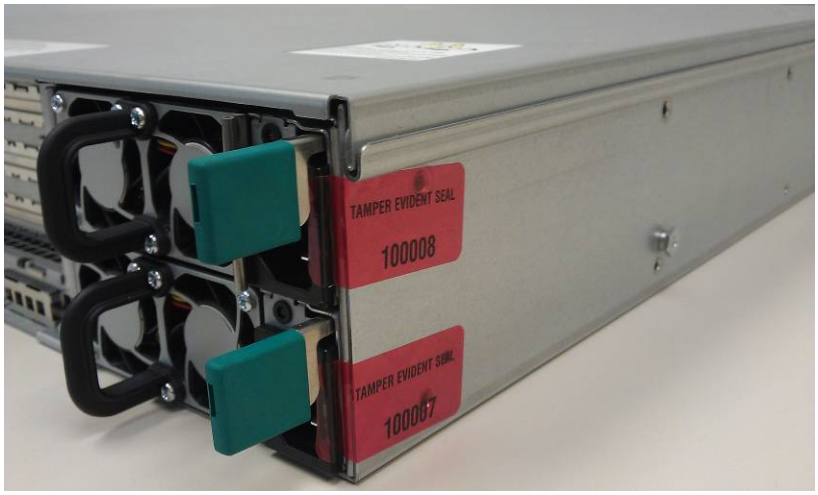


Figure 8 – Model 5500 Power Supply Seal Placement

3.2 User Guidance

The User must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

End of Document
