McAfee, Inc.

Firewall Enterprise Control Center

Hardware Version: FWE-C1015, FWE-C2050, FWE-C3000
Firmware Version: 5.3.2 Patch 6

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.14

Prepared for:

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
United States of America

Phone: +1 888 847 8766
Email: info@mcafee.com
http://www.mcafee.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Firewall Enterprise Control Center from McAfee, Inc. This Security Policy describes how the Firewall Enterprise Control Center meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The Firewall Enterprise Control Center is referred to in this document as Control Center crypto-module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The McAfee website (http://www.mcafee.com) contains information on the full line of products from McAfee.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to McAfee. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to McAfee and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact McAfee.

2 Firewall Enterprise Control Center

2.1 Overview

Firewall Enterprise Control Center provides a central interface for simplifying the management of multiple McAfee Firewall Enterprise appliances.

Control Center enables scalable centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates, inventory their firewall products, generate reports, and demonstrate regulatory compliance. The Control Center solution allows network administrators to fully mange their firewall solutions from the network edge to the core.

Control Center can also be used to centrally monitor Firewall Enterprise audit stream data, providing a high level overview of network activity and behavior, which can be further filtered to individual appliances, devices, groups, and users. For geographically diverse or multi-tenant deployments, Control Center allows network administrators to define Configuration Domains, and segment firewall policies between them.

Network administrators access Control Center server functionality in several ways. Primary management of the solution is done via the Control Center Client Application (also referred as GUI[1]), which is designed to run on an administrator's workstation. Additionally, subsets of management functionality including reporting and status monitoring are exported to McAfee's ePolicy Orchestrator via a common Application Programming Interface (API).

2.1.1 Firewall Enterprise Control Center Appliances

McAfee offers three variations of Firewall Enterprise Control Center hardware appliances. The lower end C1015 Control Center is a 1U chassis and is capable of managing up to fifteen Firewall Enterprise appliances. The C2050 Control Center appliance is a 1U chassis with a RAID[2]1 hard drive configuration and is capable of managing up to fifty Firewall Enterprise appliances. Lastly, the C3000 Control Center appliance is a 1U chassis with a RAID5 hard drive configuration and is capable of managing 100 Firewall Enterprise appliances. The C3000 is also upgradable to manage an unlimited number of Firewall Enterprise appliances.

Firewall Enterprise Control Center is also available as a virtual appliance, capable doing everything the physical hardware appliances can do. A separate Security Policy is available for the Control Center Virtual Appliance detailing how it meets the security requirements of FIPS PUB 140-2.

2.1.2 Architecture Overview

The Control Center Server firmware is hosted on McAfee Linux Operating System (MLOS) v2.2.3. The firmware is divided into five components which represent distinct functionality of the Control Center Server:

- Auditing – Control Center can store audit data both locally in the file system and remotely on a secure Syslog server. Configuration of auditing behavior is conducted by an administrator using the Control Center Client Application.

[1] GUI – Graphical User Interface
[2] RAID – Redundant Array of Independent Disks

- Tomcat – Tomcat is used to facilitate communication between the Control Center server and its Client Application or firewalls within its domain.
- Database – A PostgreSQL database used to store policy and configuration data.
- DCS – The Data Collection Server (DCS) is used to gather alerts from the Control Center and the firewalls. The UTT[3] client of the firewall sends alerts over an SSL connection to the UTT server listening on port 9006.
- Control Center Features – The management functionality provided to the Control Center Client includes Control Center Server and firewall backup and restore operations, provisioning of configuration domains and HA[4] topologies, firmware updates, the ePolicy Orchestrator extension, and the security event manager.

Figure 1 shows the basic architecture of a Control Center deployment. The red dotted line indicates the cryptographic module boundary.

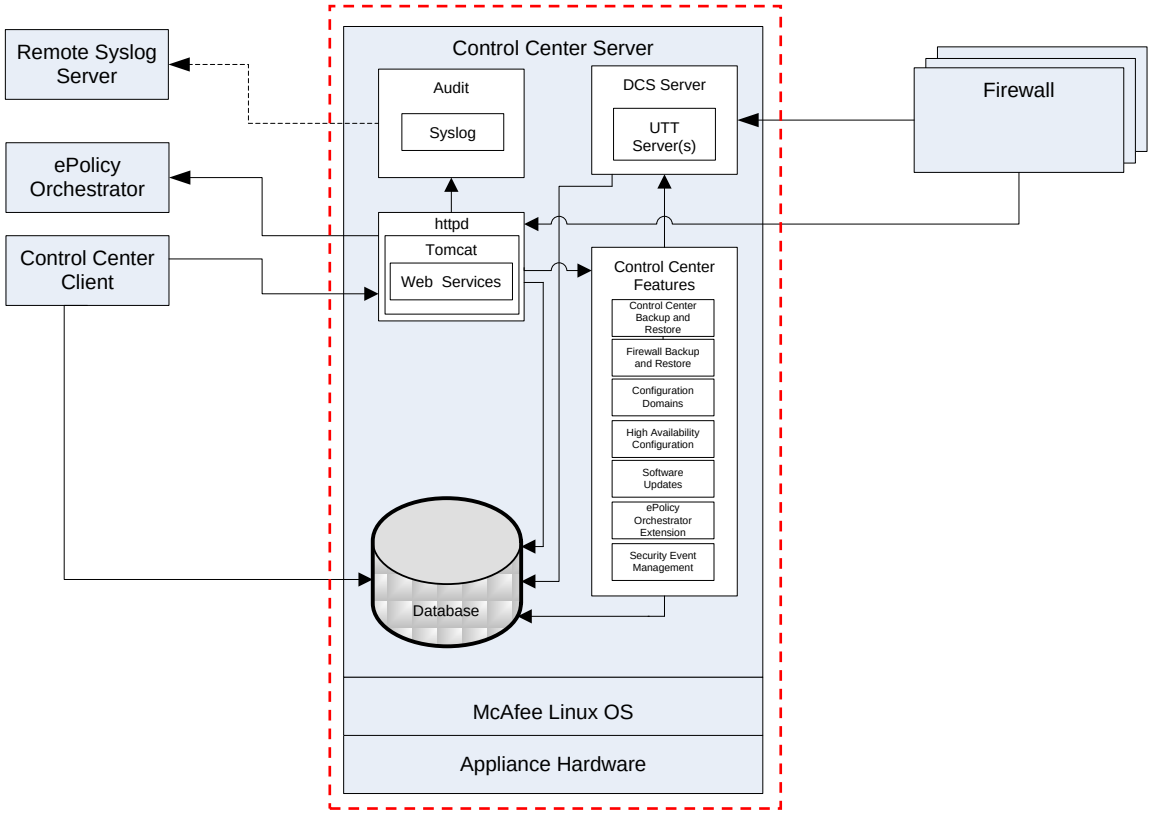

Figure 1 – Firewall Enterprise Control Center Architecture[5]

[3] UTT – User Datagram Protocol (UDP) over Transmission Control Protocol (TCP) Tunnel
[4] HA – High Availability
[5] httpd – hyper-text transfer protocol (HTTP) daemon

The Firewall Enterprise Control Center is validated at the following FIPS 140-2 Section levels, shown in Table 1:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[6]
7	Cryptographic Key Management	2
8	EMI/EMC[7]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Firewall Enterprise Control Center (Hardware Version: FWE-C1015, FWE-C2050, FWE-C3000) is a hardware module with a multiple-chip standalone embodiment. The overall security level of the module is level 2. The physical cryptographic boundary of the Firewall Enterprise Control Center is defined by the hard metal casing making up the physical embodiment of each individual server chassis. The dotted line in Figure 1 above indicates the cryptographic boundary of the module.

Figure 2 and Figure 3 show pictures of the FWE-C1015, FWE-C2050, and FWE-C3000 Control Centers, respectively.

Figure 2 – FWE-C1015 Control Center

Figure 3 – FWE-C2050/C3000 Control Center

[6] N/A – Not Applicable
[7] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

.

2.3 Module Interfaces

The FWE-C1015, FWE-C2050, and FWE-C3000 cryptographic modules' physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Physical interfaces for the FWE-C1015 Control Center are described in Table 2 and shown in Figure 5. The procedure for attaching the required security bezel to the front panel of the module is outlined in the Crypto Officer Guidance in Section 3 of this document. The USB[8] ports will only support Control Input while the module is running in FIPS-Approved mode of operation.

Figure 4 – FWE-C1015 Front Panel

Figure 5 – FWE-C1015 Rear Panel Physical Interfaces

Table 2 – FWE-C1015 FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
NIC[9] (10/100/1000) Ports	2	• Data Input • Data Output • Control Input • Status Output
PS/2 Port	2	• Control Input
Serial Port (DB-9)	1	• Data Input • Control Input
USB	2	• Control Input
Video Connector	1	• Status Output
LED	9	• Status Output

[8] USB – Universal Serial Bus
[9] NIC – Network Interface Controller

.

Power Interface	1	• Power Input

Physical interfaces for the FWE-C2050 and FWE-C3000 Control Centers are described in Table 3 and shown in Figure 7. Installation of the required security bezel to the front panel of the modules is described in the Crypto Officer Guidance in Section 3 of this document. The USB ports will only support Control Input while the module is running in the FIPS-Approved mode of operation.

Figure 6 – FWE-C2050/ FWE-C3000 Front Panel

Figure 7 – FWE-C2050/ FWE-C3000 Real Panel Physical Interfaces

Table 3 – FWE-C2050/ FWE-C3000 FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
NIC (10/100/1000) Ports	2	• Data Input • Data Output • Control Input • Status Output
RJ-45 Management port	1	• Control Input • Status Output
RJ-45 Serial B Connector	1	• Data Input • Data Output • Control Input • Status Output
USB	4	• Control Input
Video Connector	1	• Status Output
LED	21	• Status Output
Power Interface	2	• Power Input

A block diagram of the FWE-C1015, FWE-C2050, and FWE-C300 is provided in Figure 8 below. The figure shows the modules' physical interfaces and the associated logical interfaces.

.

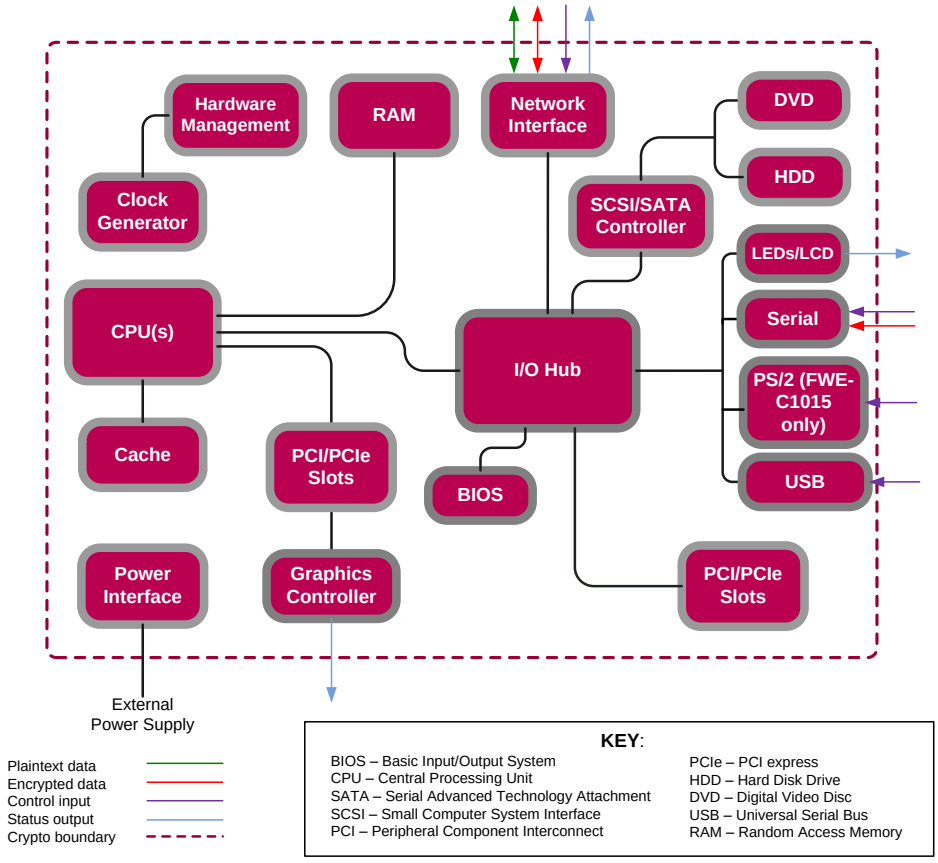

Figure 8 – FWE-C1015, FWE-C2050, and FWE-C300 Physical Interfaces

2.4 Roles and Services

The module supports role-based authentication. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role. Each role and their corresponding services are detailed in the sections below. Please note that the keys and CSPs listed in the tables indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto Officer Role

The Crypto Officer (CO) role has the ability to initialize the module for first use, run on-demand self-tests, manage operator passwords, and zeroize keys. Descriptions of the services available to the CO role are provided in Table 4 below.

.

Table 4 – CO Services

Service	Description	Input	Output	Approved Algorithms Accessed	CSP and Type of Access
Run self-tests on demand	Performs power-up self-tests	Command and parameters	Command response	N/A	None
Module Initialization	Initial configuration of the module.	Command and parameters	Command response and status output	RSA, SP800-90A DRBG	CA[10] Public/Private Key – W Web Server Public/Private Key – W PostgreSQL Public/Private Key – W DCS Public/Private Key – W SSH[11] Public/Private Keys – W CO Password – W User Password – W
Change Passwords	Change the password for the CO and internal database users	Command and parameters	Command response and status output	N/A	CO Password – R, W
Zeroize Keys	Zeroize all public and private keys and CSPs	Command and parameters	Command response and status output	N/A	All keys – W
Access CLI[12] Services[13]	Access the CLI over Ethernet port or serial port to configure or monitor status of the module	Command and parameters	Command response and status output	RSA, DSA, SHA, HMAC	CO Password – X SSH Public/Private Key – R, X SSH Authentication Key – R, X SSH Session Key – W, X

2.4.2 User Role

The User role has the ability to manage the Control Center through the Control Center Client Application. Services available through the application include modifying the RADIUS[14] and LDAP[15] configuration and connecting to a specified firewall. Descriptions of the services available to the User role are provided in the Table 5 below.

[10] CA – Certificate Authority
[11] SSH – Secure Shell
[12] CLI – Command Line Interface
[13] The SSH protocol has not been reviewed or tested by the CAVP or CMVP
[14] RADIUS – Remote Authentication Dial In User Service
[15] LDAP – Lightweight Directory Access Protocol

.

Table 5 – User Services

Service	Description	Input	Output	Approved Algorithms Accessed	CSP and Type of Access
Create System Backup File	Create a restoration backup file	Command and parameters	Command response and status output	N/A	None
Restore System	Restore the system with a system backup file	Command and parameters	Command response and status output	N/A	None
RADIUS Services	Configure and manage RADIUS server authentication mechanisms	Command and parameters	Command response	N/A	RADIUS credential – W, R, X
LDAP Services	Configure and manage LDAP server authentication mechanisms	Command and parameters	Command response	N/A	LDAP Credential – W, R, X
Firewall Services	Establish connection to the Firewall and Firewall management.	Command and parameters	Command response	RSA, DSA, AES, Triple-DES, SHA, HMAC	CA Private Key – X CA Public Key – X DCS Private Key – X DCS Public Key – X SSH Public Key – X SSH Private Key – X SSH Authentication Key – X SSH Session Key – W, X
Change User Password	Change the password of the User	Command and parameters	Command response and status output	N/A	User Password – R, W
Show Status	Show status of the module	Command and parameters	Command response and status output	N/A	None

.

Service	Description	Input	Output	Approved Algorithms Accessed	CSP and Type of Access
Access GUI[16] services[17]	Access the GUI over Ethernet port to configure or monitor status of the module	Command and parameters	Command response and status output	RSA, AES, Triple-DES	User Password – X CA Private Key – X CA Public Key – X Web Server Public/ Private Key – X Web Server Session Key – W, X PostgreSQL Public/Private Key – X PostgreSQL Session Key – W, X

2.4.3 Non-Security Relevant Services

The module offers additional services to both the CO and User, which are not relevant to the secure operation of the module. All services provided by the modules are listed in the *McAfee Firewall Enterprise Control Center 5.3.2 Product Guide; Revision A (2013)*. The product guide is supplied with the shipment of the Control Center modules or may be freely obtained at http://www.mcafee.com/us/downloads/downloads.aspx.

2.4.4 Authentication

The Control Center devices support role-based authentication to control access to services that require access to sensitive keys and CSPs. To perform these services, an operator must log in to the module by authenticating with the respective role's username and secure password. The CO and User passwords are initialized by the CO as part of module initialization, as described in Section 3 (Secure Operation) of this document. Once the operator is authenticated, they will assume their respective role and carry out the available services listed in Table 4 and Table 5. All users authenticate to the module using User-ID and passwords.

2.4.4.1 Authentication Data Protection[18]

The module does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Authentication data can only be modified by the operator who has assumed the CO role or User role with administrator privileges. The module hashes the operator's password with an MD5 hash function and stores the hashed password in a password database.

2.4.4.2 Authentication Mechanism Strength

Please refer to Table 6 for information on authentication mechanism strength:

[16] GUI – Graphical User Interface
[17] The Transport Layer Security (TLS) protocol has not been reviewed or tested by the CAVP or CMVP
[18] "Protection" does not imply cryptographic protection

.

Table 6 – Authentication Mechanism Strength

Role	Authentication Type	Authentication Strength
Crypto Officer or User	Password	The minimum length of the password is eight characters and is enforced by this Security Policy (see Section 3.1.4). A total of 95 different case-sensitive, alphanumeric characters and symbols can be used (including the 'space' character). The chance of a random attempt falsely succeeding is 1: (95^8), or 1: 6,634,204,312,890,625. The fastest network connection supported by the module is 1000 Mbps. Hence at most ($1000x10^6 \times 60 = 6x10^{10}$ =) 60,000,000,000 bits of data can be transmitted in one minute. Each password is 64 bits, meaning $9.375x10^8$ passwords can be passed to the module (assuming no overhead). This equates to a 1:7,076,484 chance of passing in the correct password in a one minute period.

2.5 Physical Security

The Firewall Enterprise Control Center is a multi-chip standalone cryptographic module. The module consists of production-grade components that include standard passivation techniques. The chassis of the Control Center modules is made of hard metal, which is opaque within the visible spectrum. During initial setup, the CO is required to install the security baffles that are available as part of the FIPS kit. Once the baffles are installed, all ventilation holes present on the module do not disclose any security-relevant components when inspected.

The modules contain removable covers which are protected by tamper-evident seals. The modules contain a removable, lockable front bezel. For added protection, the front bezel is secured with tamper-evident seals. Finally, the FWE-C2050 and FWE-C3000 models contain two removable power supplies that are protected by tamper-evident seals.

Please refer to the CO guidance in Section 3 (Secure Operation) of this document for guidance on the correct placement of the front security bezel, the security baffles, and the tamper-evident seals.

2.6 Operational Environment

The C1015 module is hosted on an Intel® Server System SR1530SH. The server system is a 1U system that supports the Intel® Server Board S3200SHL with an Intel® Celeron® dual core processor running MLOS 2.2.3. The server environment is a non-modifiable operational environment.

The C2050 and C3000 modules are hosted on an Intel® Server System SR1625URSAS. The server system is a 1U system that supports the Intel® Server Board S5520UR with an Intel® Xeon® quad core processor running MLOS 2.2.3. The server environment is a non-modifiable operational environment.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 7 and Table 8 below.

.

Table 7 – Crypto-J FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES[19] – ECB[20], CBC[21], CFB[22](128), OFB[23]: 128, 192 and 256 bit key sizes	2972
Triple-DES[24] – ECB, CBC, CFB(64), OFB: KO[25] 1	1761
RSA ANSI[26] X9.31, PKCS[27]#1(v1.5, 2.1) Signature Generation/Verification – 2048- and 3072-bit	1561
RSA[28] ANSI X9.31 Key Generation – 2048- and 3072	1561
DSA[29] Key Generation – 2048-bit	885
DSA PQG Parameter Generation/Verification – 2048-bit	885
DSA Signature Generation/Verification – 2048-bit	885
SHA[30]-256, SHA-384, SHA-512	2498
HMAC[31] SHA-256, HMAC SHA-384, HMAC SHA-512	1884
SP[32] 800-38C based CCM[33]	2972
SP 800-38D based GCM[34]	2972
SP800-90 HMAC DRBG	566

Table 8 – OpenSSL FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES – ECB, CBC, CFB(8), CFB(128), OFB, : 128, 192, and 256 bit key sizes	3116
Triple-DES – ECB, CBC, CFB(8), CFB(64), OFB: KO1	1787
DSA Key Generation: 2048-bit	900
DSA Signature Generation/Verification: 2048-bit	900
RSA FIPS 186-4 Key Generation: 2048- and 3072-bit	1587

[19] AES – Advanced Encryption Standard
[20] ECB – Electronic Code Book
[21] CBC – Cipher Block Chaining
[22] CFB – Cipher Feedback
[23] OFB – Output Feedback
[24] DES – Data Encryption Standard
[25] KO – Keying Option
[26] ANSI – American National Standards Institute
[27] PKCS – Public-Key Cryptography Standards
[28] RSA – Rivest, Shamir, and Adleman
[29] DSA – Digital Signature Algorithm
[30] SHA – Secure Hash Algorithm
[31] HMAC – (keyed) Hash-based Message Authentication Code
[32] SP – Special Publication
[33] CCM – Counter with Cipher Block Chaining-Message Authentication Code
[34] GCM – Galois/Counter Mode

Algorithm	Certificate Number
RSA (FIPS 186-4) ANSI X9.31, PKCS #1.5, PSS signature generation – 2048- and 3072-bit	1587
RSA (FIPS 186-4) ANSI X9.31, PKCS #1.5, PSS signature verification – 1024-, 2048-, and 3072-bit	1587
RSA (FIPS 186-2) ANSI X9.31, PKCS #1.5, PSS signature verification – 1024-, 2048-, 3072-, and 4096-bit	1587
SHA-256, SHA-384, SHA-512	2572
HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	1953
SP800-90A HASH DRBG	627

The cryptographic module implements the TLS and SSH secure networking protocols. Each protocol implements a Key Derivation Function (KDF) listed in NIST SP 800-135rev1 and has been validated by the CMVP. There certificate numbers are provided in Table 9. The complete protocol implementations have not been reviewed or tested by the CAVP[35] and CMVP.

Table 9 – Network Protocol Component Validation

Algorithm	CVL Certificate Number
TLS[36] 1.0/1.1 and TLS 1.2 KDF using SHA 256 and SHA 384	378
SSH KDF using SHA-256, -384, and -512	378

The module utilizes the following non-compliant algorithm implementations, which are allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman 2048 bits key (Key agreement/key establishment methodology provides 112 bits of encryption strength)
- SP 800-90A HASH DRBG (non-compliant) – Used for seeding approved DRBGs listed in Table 7 and Table 8.

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementations allowed for use in a FIPS-Approved mode of operation:

- RSA 2048-bit or 3072-bit key encrypt/decrypt (key establishment methodology provides 112 or 128 bits of encryption strength)
- MD5[37] for hashing passwords; creating SCEP[38] fingerprint

Caveat: Additional information concerning 2-key Triple-DES, SHA-1, Diffie-Hellman key agreement/key establishment, RSA key signatures, RSA key transport, and two-key Triple-DES and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

[35] CAVP – Cryptographic Algorithm Validation Program
[36] TLS – Transport Layer Security
[37] MD – Message Digest
[38] SCEP – Simple Certificate Enrollment Protocol

.

The module supports the critical security parameters (CSPs) listed below in Table 10

Table 10 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
CA Public Key	RSA-2048 Public key	Generated internally during module installation process	Exits the module in plaintext	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	The CA public key is used for TLS client certificate authentication
CA Private Key	RSA-2048 Private key	Generated internally during module installation process	Never exits the module	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used to sign certificates that are used by various components (such as the web server and DCS) of the module. It is also used to sign firewall certificates during firewall registration (SCEP) process. The CA private key is used to decrypt the secret key contained in digital envelope sent by a firewall to the module during SCEP. The private key is used to sign digital envelope sent by the module to the firewall during SCEP
Web Server Public Key	RSA-2048 Public key	The module's public key is generated internally during module installation process; a peer's public key enters the module in plaintext within a certificate	Exits the module in plaintext	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used for TLS server authentication
Web Server Private Key	RSA-2048 Private key	Generated internally during module installation process	Never exits the module	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used for TLS server authentication

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Web Server Session Key	TLS session key (AES-256, AES-128, Triple-DES)	Generated internally during the TLS handshake	Never exits the module	Stored inside the volatile memory in plaintext, inside the module	Zeroized on session termination as well as when the module firmware is reinstalled	It is used for encrypting/decrypting the inbound and outbound traffic during the TLS session
PostgreSQL Public Key	RSA-2048 Public key	The module's public key is generated internally; a peer's public key enters the module in plaintext within a certificate	Exits the module in plaintext	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used by the PostgreSQL server for TLS Server authentication
PostgreSQL Private Key	RSA-2048 Private key	Generated internally during module installation process	Never exits the module	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used by the PostgreSQL server for TLS Server authentication
PostgreSQL Session Key	TLS session key (AES-256, AES-128, Triple-DES)	Generated internally during the TLS handshake	Never exits the module	Stored inside the volatile memory in plaintext, inside the module	Zeroized on session termination as well as when the module is reinstalled	It is used for encrypting/decrypting the inbound and outbound traffic during the TLS session
DCS Public Key	RSA-2048 Public key	The module's public key is generated internally; a peer's public key enters the module in plaintext within a certificate	Exits the module in plaintext	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used by the UTT server for authentication with firewalls
DCS Private Key	RSA-2048 Private key	Generated internally during module installation process	Never exits the module	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used by the UTT server for TLS authentication with firewalls

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Public Key	RSA-2048 or DSA-2048 bit Public key	The module's public key is generated internally; a peer's public key enters the module in plaintext during the initial connection	Exits the module in plaintext	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used by the SSH server to authenticate itself for incoming connections
SSH Private Key	RSA-2048 or DSA-2048 bit Private key	Generated internally during module installation process	Never exits the module	Stored on disk in plaintext, inside the module	Zeroized when the module firmware is reinstalled	It is used by the SSH server for server authentication
SSH Authentication Key	HMAC SHA-256	Generated internally	Never exits the module	Stored inside the volatile memory in plaintext, inside the module	Zeroized on session termination as well as when the module firmware is reinstalled	It is used for data authentication during SSH sessions
SSH Session Key	AES-256, AES-192, AES-128, Triple-DES	Generated internally	Never exits the module	Stored inside the volatile memory in plaintext, inside the module	Zeroized on session termination as well as when the module firmware is reinstalled	It is used for encrypting/decrypting the data traffic during the SSH session
CO or User Password	Passphrase	Entered by a CO or User locally or over secure TLS channel	Never exits the module	Stored on disk in plaintext, inside the module	Zeroized when the password is updated with a new one or when the module firmware is reinstalled	Used for authenticating all COs (over CLI) and Users (over GUI)

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RADIUS credential	Alpha-numeric string	Entered by a User over GUI	Never exits the module	Stored on database in plaintext, inside the module	Zeroized when the module firmware is reinstalled	This password is used by the module to authenticate itself to the RADIUS server. This password is required for the module to validate the credential supplied by the user with the RADIUS server
LDAP credential	Alpha-numeric string	Entered by a User over GUI	Never exits the module	Stored on database in plaintext, inside the module	Zeroized when the module firmware is reinstalled	This password is used by the module to authenticate itself to the LDAP server. This password is required for the module to validate the credential supplied by the user with the LDAP server
HASH DRBG 'C' Value	Internal state value	Internally Generated	Never	Plaintext in volatile memory	Unload module; API call; Remove Power	Internal state value used by HASH DRBG
HASH DRBG 'V' value	Random value	Generated internally	Never exits the module	Volatile memory in plaintext	By process termination	Used in the process of generating a random number
HASH DRBG seed	Random Value	Generated internally by non-compliant DRBG	Never exits the module	Volatile memory in plaintext	By power cycle	Used to seed the DRBG
HMAC DRBG key value	Random value	Generated internally	Never exits the module	Volatile memory in plaintext	By process termination	Used in the process of generating a random number
HMAC DRBG seed	Random Value	Generated internally by non-compliant DRBG	Never exits the module	Volatile memory in plaintext	By power cycle	Used to seed the DRBG
HMAC DRBG 'V' value	Random value	Generated internally	Never exits the module	Volatile memory in plaintext	By process termination	Used in the process of generating a random number
Integrity test key	HMAC SHA-256 key (Shared secret)	Hardcoded	Never exits the module	Plaintext in hard drive	Not Applicable	Used to perform the firmware integrity test

2.8 Self-Tests

The Control Center appliances implement two cryptographic libraries in their firmware. The libraries, acting independently from one another, perform various Self-Tests (Power-Up Self-Tests and Conditional Self-Tests) to verify their functionality and correctness.

2.8.1 Power-Up Self-Tests

Power-Up Self-Tests are carried out every time the module is booted. Upon successful completion of the Power-Up Self-Tests, the success is printed in the log files as "Completed FIPS 140 self checks successfully" and then the module will transition to normal operation. Should either of the independent library's Power-Up Self-Test fail, the module will enter an error state and the library will cause the module to cease operation. While in this error state, the module will log and display the critical error (for User's and CO's review) and will inhibit all cryptographic operations and data output by disabling all data output interfaces and then coming to a halt. To recover, the CO can shutdown or restart the module and attempt the boot sequence again. If the module continually enters this state, the CO must reinstall the firmware with the supplied materials.

The Firewall Enterprise Control Center performs the following self-tests at power-up:

- Firmware integrity check (HMAC SHA-256)
- Approved Algorithm Tests
    - Crypto-J AES Encrypt KAT[39]
    - Crypto-J AES Decrypt KAT
    - OpenSSL AES Encrypt KAT
    - OpenSSL AES Decrypt KAT
    - Crypto-J AES GCM Encrypt KAT
    - Crypto-J AES GCM Decrypt KAT
    - Crypto-J Triple-DES KAT
    - OpenSSL Triple-DES KAT
    - Crypto-J RSA KAT
    - OpenSSL RSA KAT
    - Crypto-J DSA pair-wise consistency test
    - OpenSSL DSA pair-wise consistency test
    - Crypto-J SHA-256 KAT
    - OpenSSL SHA-256 KAT
    - Crypto-J SHA-384 KAT
    - OpenSSL SHA-384 KAT
    - Crypto-J SHA-512 KAT
    - OpenSSL SHA-512 KAT
    - Crypto-J HMAC SHA-256 KAT
    - OpenSSL HMAC SHA-256 KAT
    - Crypto-J HMAC SHA-384 KAT
    - OpenSSL HMAC SHA-384 KAT
    - Crypto-J HMAC SHA-512 KAT
    - OpenSSL HMAC SHA-512 KAT
    - Crypto-J SP800-90 HMAC DRBG KAT
    - OpenSSL SP800-90A HASH DRBG KAT

[39] KAT – Known Answer Test

2.8.2 Conditional Self-Tests

Conditional Self-Tests are run on as needed by the module. When a Conditional Self-Test passes, the module will continue with normal operation. If the OpenSSL or Crypto-J library incurs a failure during a Conditional Self-Test, the module will enter a soft error state. The module is capable of recovering from the soft error without a user's intervention.

The Firewall Enterprise Control Center performs the following conditional self-tests:

- OpenSSL HASH DRBG Continuous RNG test
- Crypto-J HMAC DRBG Continuous RNG test
- Non-compliant DRBG Continuous RNG test
- Crypto-J RSA pair-wise consistency test
- OpenSSL RSA pair-wise consistency test
- Crypto-J DSA pair-wise consistency test
- OpenSSL DSA pair-wise consistency test
- Firmware upgrade test with DSA signature verification

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

The Firewall Enterprise Control Center meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 CO and User Guidance

The CO shall be in charge of receiving, installing, initializing, and maintaining the Control Center modules. The CO shall take assistance (when required) from an authorized User during the initial setup of the module. A CO or User must be diligent to follow complex password restrictions and must not reveal their password to anyone. The CO shall reinstall the module firmware if the module has encountered a critical error and the module is non-operational. A User is recommended to reboot the module if the module ever encounters any soft errors. The following sections provide important instructions and guidance to the CO for secure installation and configuration of the Control Center.

3.1.1 Initial Setup

Upon receiving the Control Center hardware, the CO shall check that the appliance is not damaged and that all required parts and instructions are included. The Control Center will be shipped with the following items:

- Front Bezel
- Mountain Rails
- Mounting ears (2) and associated screws (4)
- Cable Management Arm (C2050, C3000)
- (1) Power cord (C1015)
- (2) Power cords (C2050, C3000)
- RJ-45 to DB-9 Female Serial Cable (C2050, C3000)
- Firewall Enterprise Control Center 5.x USB Flash Drive
- McAfee Diagnostic USB Flash Drive
- Firewall Enterprise Control Center 5.x Client CD
- Firewall Enterprise Control Center 5.x Server CD
- FIPS Kit for C1015 (Part #: FWE-CC-FIPS-KIT1)
- FIPS Kit for C2050 or C3000 (Part #: FWE-CC-FIPS-KIT2)
- Multilingual installation/setup guides, warranty information, and other helpful materials

Installation of the security baffles, front security bezel, and tamper-evident seals is required in order to operate the module in the FIPS-Approved mode of operation. The CO shall follow the included instructions for secure installation of the modules into a rack system after placement of the security baffles and tamper-evident seals.

3.1.1.1 Security Baffle Installation

In order to provide additional security, security baffles shall be installed by the CO prior to placing the tamper-evident seals onto the module chassis. Security baffles installation instructions are available to the CO as part of the FIPS Kit. Each appliance requires one (1) security baffle.

Figure 9 shows the FWE-C1015 cryptographic module with the security baffles installed in the rear of the module.

.

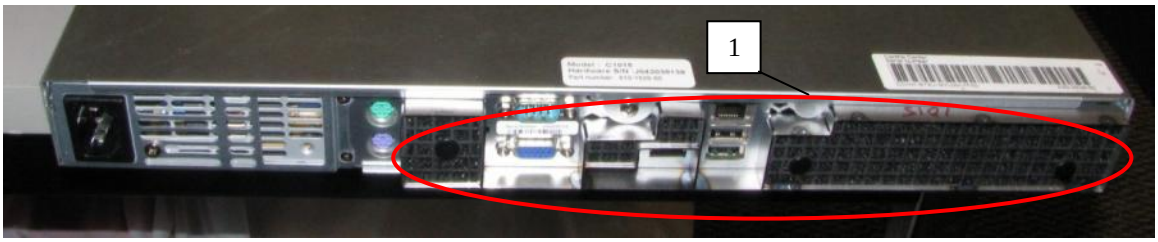

Figure 9 – FWE-C1015 Security Baffle Placement

Figure 10 shows the FWE-C2050 cryptographic module with the security baffles installed in the rear of the module.

Figure 10 – FWE-C2050 Security Baffle Placement

Figure 11 shows the FWE-C3000 cryptographic module with the security baffles installed in the rear of the module.

Figure 11 – FWE-C3000 Security Baffle Placement

3.1.1.2 Installation of Secure Front Bezel

The front bezel, pictured in Figure 4 and Figure 6 in Section 2.3 will prevent operators of the Control Center modules from accessing the front USB port and power button of all devices, in addition to the DVD[40] drive and ID[41] button on the C2050 and C3000. To install the front bezel, the CO shall refer to the guide included in the Control Center shipment materials. Access to the front panel of any of the modules shall be limited to the CO during initial module configuration.

3.1.1.3 Placement of Tamper-Evident Seals

McAfee Firewall Enterprise Control Center uses tamper-evident seals to protect against unauthorized access to within the modules through the removable covers. These seals are shipped as part of the FIPS Kit. If one of the seals shows evidence of tampering, it is possible the module has been compromised. It is up to the CO to ensure proper placement of the tamper-evident seals using the following steps:

- Apply at room temperature – the adhesive will not form a solid bond if applied at temperatures below 50° F.
- The surface must be dry and free of dirt, oil, and grease, including finger oils. Alcohol pads can be used.

[40] DVD - Digital Video Disc
[41] ID - Identification

- Place the seal and rub thumb over it to ensure complete adhesion
- Wait 72 hours to ensure a complete adhesive bond. This will ensure that all tamper-evident features of the seals can be activated

Maintenance of the tamper-evident seals is the responsibility of the CO. The tamper-evident seals must be inspected periodically by the CO for tamper evidence. If the CO finds evidence of tampering, then the module is no longer FIPS compliant. The CO shall maintain control of any unused/additional tamper-evident seals after installation of the seals is complete.

3.1.1.3.1 C1015 Tamper-Evident Seal Placement

Placement of the tamper-evident seals for the C1015 is shown in Figure 12 and Figure 13. Two (2) tamper-evident seals will be used in total for this appliance. Figure 12 shows the seal placement on top of the appliance. The seal is to be placed on both the metal chassis and on the security bezel. It is important to note that the placement of the sticker on the top of the chassis is covering one of the screw heads holding the top plate in place. This will ensure that evidence of trying to access the top plate is clearly visible.

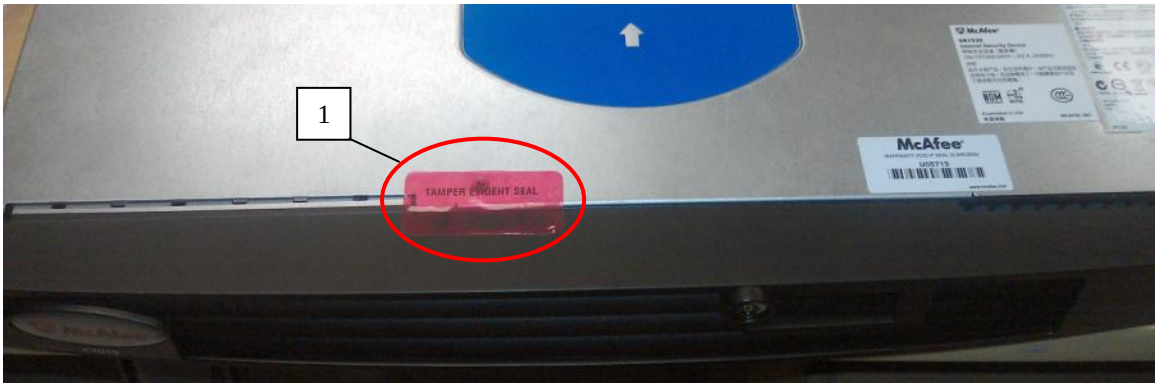

Figure 12 – FWE-C1015 Tamper-Evident Seal Placement (Top)

.

Figure 13 shows seal placement on the bottom of the appliance. This seal is to be placed on both the metal chassis and the security bezel. By placing the tamper-evident seals on both the top and bottom of the security bezel, this ensures that the bezel cannot be removed from either side of the chassis.

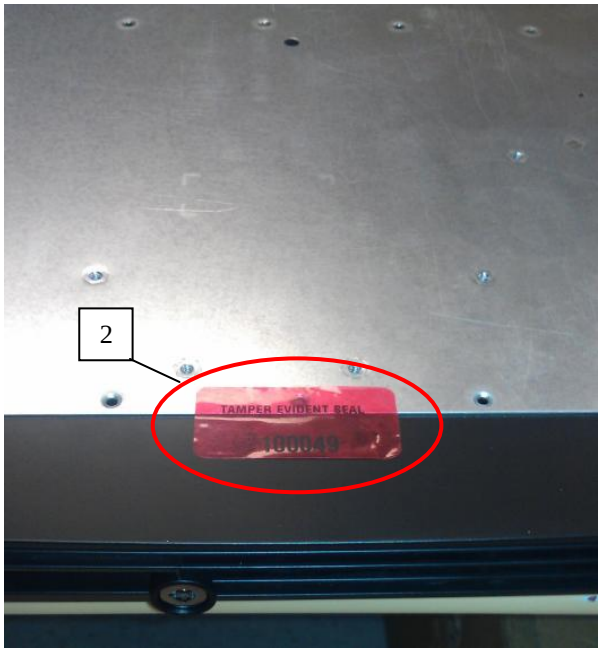

Figure 13 – FWE-C1015 Tamper-Evident Seal Placement (Bottom)

3.1.1.3.2 C2050/C3000 Tamper-Evident Seal Placement

Placement of the tamper-evident seals for the C2050 and C3000 is shown in Figure 14, Figure 15, and Figure 16. The C2050 and C3000 will each require five (5) tamper-evident seals. Figure 14 shows the seal placement on top of the appliance. Tamper-evident seal #1 is placed between the removable top cover of the chassis and the chassis itself. This ensures that any attempt to remove the top panel of the appliance will show evidence of tampering. Tamper-evident seal #2 is placed on both the chassis and the front security bezel.

.

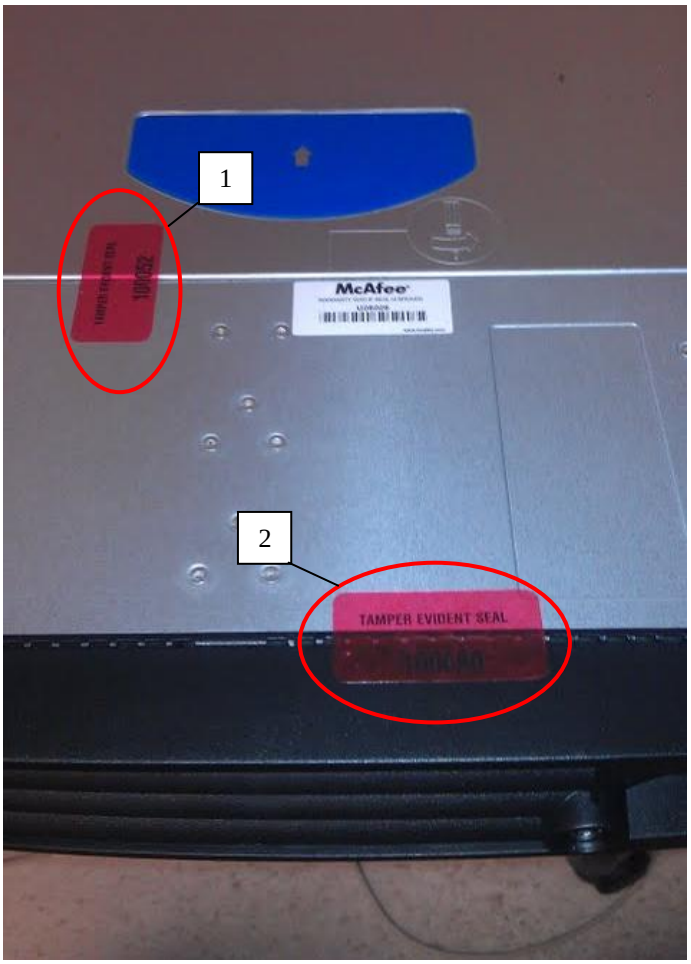

Figure 14 – FWE-C2050/ FWE-C3000 Tamper-Evident Seal Placement (Top)

.

Figure 15 shows seal placement on the bottom of the appliance. This seal is to be placed on both the metal chassis and the security bezel. By placing the tamper-evident seals on both the top and bottom of the security bezel, this ensures that the bezel cannot be removed from either side of the chassis.

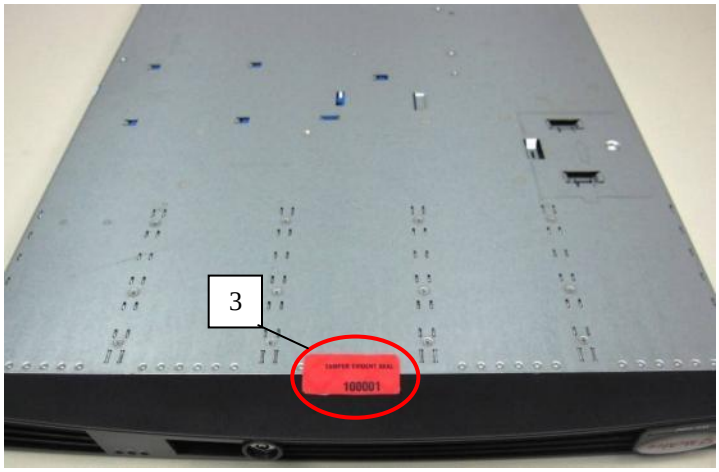

Figure 15 – FWE-C2050/ FWE-C3000 Tamper-Evident Seal Placement (Bottom)

Figure 16 shows the tamper-evident seal placement for the removable power supplies. Seals will be placed on the bottom of the Control Center chassis and wrapped around to cover the removable power supplies.

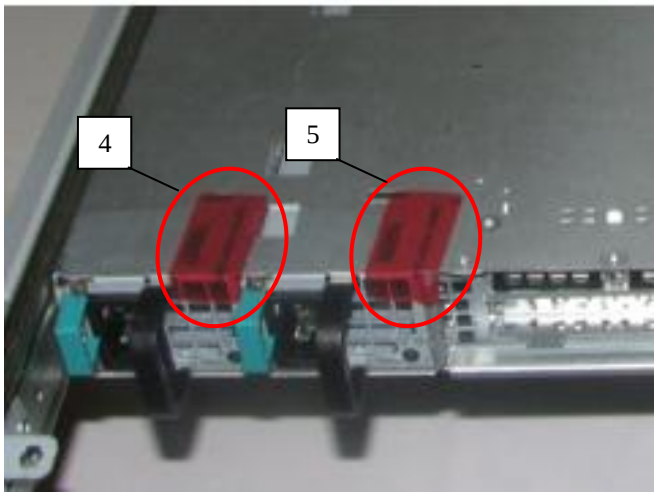

Figure 16 – FWE-C2050/ FWE-C3000 Power Supply Tamper-Evident Seal Placement (Bottom)

3.1.2 Initialization

The CO shall refer to the "Planning and setup" section of the *McAfee Firewall Enterprise Control Center: Product Guide* when preparing to setup Control Center in a network environment.

After the module has booted up and run through its initial setup, there will be a message on the screen stating that the module cannot find a configuration file. The CO shall choose to manually configure the Control Center with network settings.

Once the Control Center network settings have been fully configured, it will reboot and then give the prompt for the CO (Administrator account) to login. When this prompt appears, the appliance has been properly configured.

3.1.3 Configure FIPS settings

The Control Center is shipped and initially operates with FIPS settings not configured. The following instructions must be followed to ensure the module operates in a FIPS-Approved mode of operation.

NOTE: This is a one-way operation. Once the module has been configured for FIPS mode, the module must be completely reset and reinitialized (by reinstalling the firmware) in order to bring it back to its pre-configured state.

3.1.3.1 Install Control Center Software

The CO shall first install the Firewall Enterprise Control Center firmware onto the Firewall Enterprise Control Center appliances. The CO must obtain Firmware Version: 5.3.2 Patch 6 from McAfee and then follow the instructions in the "Install Control Center software" section of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuration Guide*. After installing the module firmware, the CO shall continue to configure the module's BIOS.

3.1.3.2 Configure the BIOS[42]

Once the module is securely installed and initialized per the instructions provided in Sections 3.1.1 and 3.1.2 of this Security Policy, the CO must follow the instructions outlined in the "Modify Bios Settings" section of the *McAfee Firewall Enterprise Control Center Installation Guide FIPS 140-2 Level 2 Kit* to configure and password protect the BIOS. Once the BIOS has been configured, the CO shall save all changes and exit. The appliance will reboot and the CO shall continue to configure the module for the FIPS-Approved mode.

3.1.3.3 Turning On FIPS Cryptography

Under supervision of the CO, the User must enable FIPS cryptography through the Firewall Control Center Client Application. Turning on FIPS cryptography means that the system will use FIPS-Approved cryptographic libraries and keys. Instructions can be found in the "Enable FIPS 140-2 processing" section of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuration Guide.*

3.1.3.4 Enabling FIPS-Approved Mode

In the FIPS-Approved Mode, FIPS-Approved cryptographic libraries are used, keys comply with FIPS-Approved lengths, and FIPS self-tests are run. Root access and other OS-level accounts cannot login after the FIPS-Approved mode is enabled. Detailed instructions for enabling the FIPS-Approved Mode can be found in the "Place the Control Center in FIPS mode" section of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuration Guide*. This process will replace all CSPs, certificates, and SSH server keys and block access to all OS-level accounts, except for the Administrator account (CO account).

3.1.3.5 Changing CO and User Passwords

The CO shall change the CO and User passwords after configuring the module for the FIPS-Approved mode. Instructions for changing the CO and User passwords are provided in the "Reset database user passwords and operating system-level user passwords" and "Reset the Control Center administrator password" sections of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuration Guide*. The CO shall follow the password management policy provided in Section 3.1.4 of this Security Policy.

[42] BIOS – Basic Input Output System

.

3.1.3.6 Enable Control Center Backup Encryption

The last step to setting up the module for use in the FIPS-Approved mode is to enable encryption on backup files. The CO shall follow the instructions provided by the "Enable Control Center backup encryption" section of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuration Guide.* When creating a passphrase, the CO shall follow the password management policy provided in Section 3.1.4 of this Security Policy.

3.1.4 Password Management

The CO is responsible for changing CO and User passwords during module initialization as well as during normal operation. Password lengths shall be 8 characters in length, at minimum. Passwords may use any combination of upper-case and lower-case characters, numbers, and special characters (including 'space').

3.1.5 Module's Mode of Operation

After configuring Control Center using the above instructions, the module can only be operated in the FIPS-Approved mode of operation. An authorized User can access the module via the Control Center Client Application and determine whether the module is operating in the FIPS-Approved mode.

Detailed steps and procedures required to determine whether the module is operating in FIPS-Approved mode can be found in the "Verify the Control Center is in FIPS mode" section of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuration Guide*.

3.1.6 Zeroization

After the Firewall Enterprise Control Center has been placed into FIPS-Approved Mode, the CO may zeroize all keys, CSPs, and certificates by reinstalling the Control Center image onto the module. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has been completed. The CO shall then follow the steps outlined above to place the newly installed Control Center firmware image back into FIPS-Approved mode.

4 Acronyms

Table 11 defines the acronyms used in this document.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input Output System
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DCS	Data Collection Server
DSA	Digital Signature Algorithm
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DVD	Digital Video Disc
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash Message Authentication Code
httpd	hyper-text transfer protocol (HTTP) daemon
ID	Identification
KAT	Known Answer Test
KDF	Key Derivation Function

.

Acronym	Definition
KO	Keying Option
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
MLOS	McAfee Linux Operating System
N/A	Not Applicable
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OFB	Output Feedback
PKCS	Public-Key Cryptography Standards
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
SP	Special Publication
SSH	Secure Shell
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
USB	Universal Serial Bus
UTT	User Datagram Protocol (UDP) over Transmission Control Protocol (TCP) Tunnel

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com