McAfee, Inc.

Firewall Enterprise Control Center

HW Version: FWE-C1015, FWE-C2050, FWE-C3000; FW Version: 5.2.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.2

Prepared for:

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

Phone: (408) 988-3832
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: (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 Canada (CSEC) 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 set up 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 set up and is capable of managing 100 Firewall Enterprise appliances. The C3000 is also upgradable to manage an unlimited amount 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 laid out by FIPS PUB 140-2.

2.1.2 Architecture Overview

The Control Center Server firmware is hosted on CGLinux secured by McAfee using RSBAC[3], an open-source access control framework. 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
[3] RSBAC – Rule Set Based Access Control

- 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[4] client of the firewall sends alerts over an SSL connection to the UTT server of the 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[5] 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.

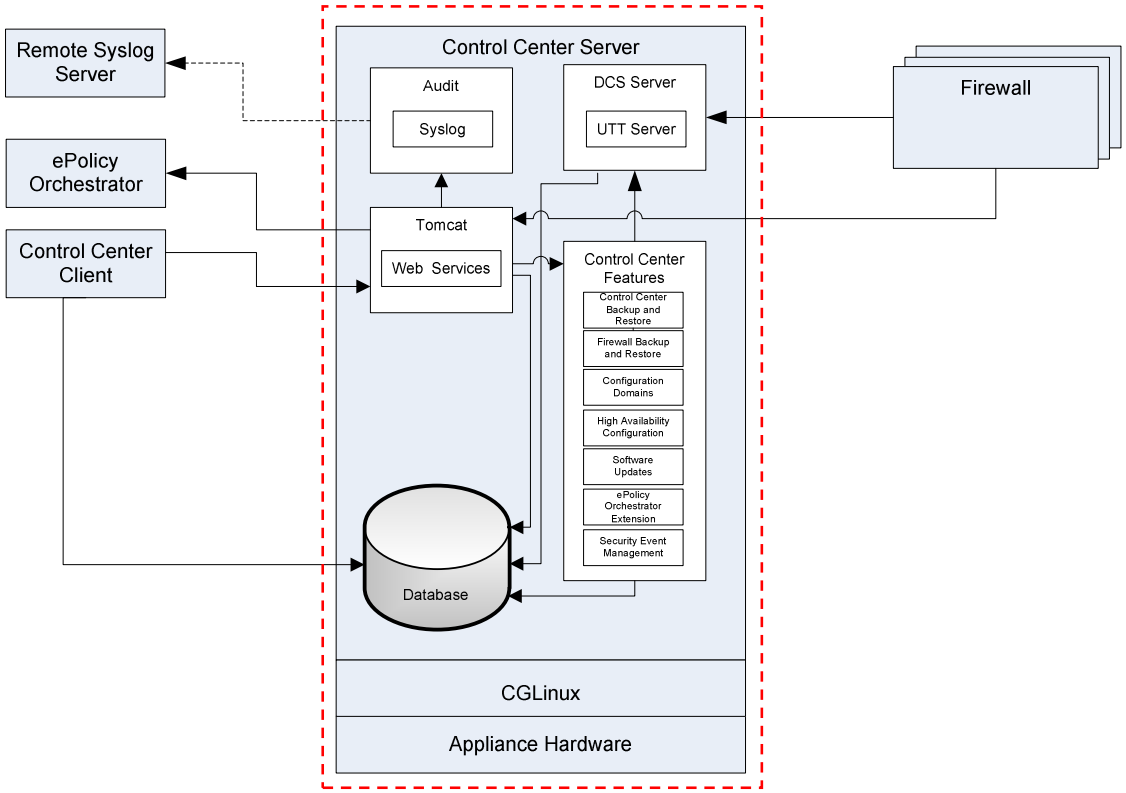

Figure 1 – Firewall Enterprise Control Center Architecture

[4] UTT – User Datagram Protocol (UDP) over Transmission Control Protocol (TCP) Tunnel
[5] HA - High Availability

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
7	Cryptographic Key Management	2
8	EMI/EMC[6]	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 (HW Version: FWE-C1015, FWE-C2050, FWE-C3000; FW Version: 5.2.0) 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 indicates the cryptographic boundary of the module.

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

Figure 2 – C1015 Control Center

Figure 3 – C2050/C3000 Control Center

[6] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.3 Module Interfaces

The C1015, C2050, and 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 C1015 Control Center are described in Table 2 and shown in Figure 4 and 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[7] ports will only support Control Input while the module is running in FIPS-Approved mode of operation.

Figure 4 – C1015 Front Panel

Figure 5 – C1015 Rear Panel Physical Interfaces

Table 2 – C1015 FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
NIC[8] (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
Power Interface	1	• Power Input

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

Physical interfaces for the C2050 and C3000 Control Centers are described in Table 3 and shown in Figure 6 and Figure 7. Attaching the required security bezel to the front panel of the modules is outlined 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 FIPS-Approved mode of operation.

Figure 6 – C2050/C3000 Front Panel

Figure 7 – C2050/C3000 Real Panel Physical Interfaces

Table 3 – C2050/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

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	CSP and Type of Access
Run self-tests on demand	Performs power-up self-tests	Command and parameters	Command response	None
Module Initialization	Initial configuration of the module.	Command and parameters	Command response and status output	CA[9] Public/Private Key – W Web Server Public/Private Key – W PostgreSQL Public/Private Key – W DCS Public/Private Key – W SSH 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	CO Password – R, W
Zeroize Keys	Zeroize all public and private keys and CSPs	Command and parameters	Command response and status output	All keys – W
Access CLI[10] Services	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	CO Password – X SSH Public/Private Key – R, X SSH Authentication Key – R, X SSH Session Key – W, X

[9] CA – Certificate Authority
[10] CLI – Command Line Interface

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[11] and LDAP[12] configuration and connecting to a specified firewall. Descriptions of the services available to the User role are provided in the Table 5 below.

Table 5 – User Services

Service	Description	Input	Output	CSP and Type of Access
Create System Backup File	Create a restoration backup file	Command and parameters	Command response and status output	None
Restore System	Restore the system with a system backup file	Command and parameters	Command response and status output	None
RADIUS Services	Configure and manage RADIUS server authentication mechanisms	Command and parameters	Command response	RADIUS credential – W, R, X
LDAP Services	Configure and manage LDAP server authentication mechanisms	Command and parameters	Command response	LDAP Credential – W, R, X
Firewall Services	Establish connection to the Firewall and Firewall management.	Command and parameters	Command response	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 Session Key – W, X
Change User Password	Change the password of the User	Command and parameters	Command response and status output	User Password – R, W
Show Status	Show status of the module	Command and parameters	Command response and status output	None
Access GUI[13] services	Access the GUI over Ethernet port to configure or monitor status of the module	Command and parameters	Command response and status output	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

[11] RADIUS – Remote Authentication Dial In User Service
[12] LDAP – Lightweight Directory Access Protocol
[13] GUI – Graphical User Interface

2.4.3 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. Users may authenticate to the module using User-ID and passwords.

2.4.3.1 Authentication Data Protection[14]

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.

2.4.3.2 Authentication Mechanism Strength

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

Table 6 – Authentication Mechanism Strength

Role	Authentication Type	Authentication Strength
Crypto Officer or User	Password	The minimum length of the password is eight characters, with 91 different case-sensitive alphanumeric characters and symbols possible for usage. The chance of a random attempt falsely succeeding is 1: (91^8), or 1: 4,702,525,276,151,521. The fastest network connection supported by the module is 100 Mbps. Hence at most ($100 \times 10^6 \times 60 = 6 \times 10^9$ =) 6,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: [(91^8) / (6×10^9)], or 1: 783,754, which is less than 1in 100,000 as required by FIPS 140-2.

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 a hard metal, 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 present or disclose any security-relevant components when inspected.

The modules contain removable covers which are protected by tamper-evident seals, as shown in Figure 8. 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 modules contain a removable,

[14] "Protection" does not imply cryptographic protection

lockable front bezel as depicted in Figure 9 below. Lastly, the C2050 and C3000 models contain two removable power supplies that are protected by tamper-evident seals, as shown in Figure 13.

Figure 8 – Control Center Tamper-Evident Seals

Figure 9 and Figure 10 show proper tamper-evident seal placement on the C1015 Control Center.

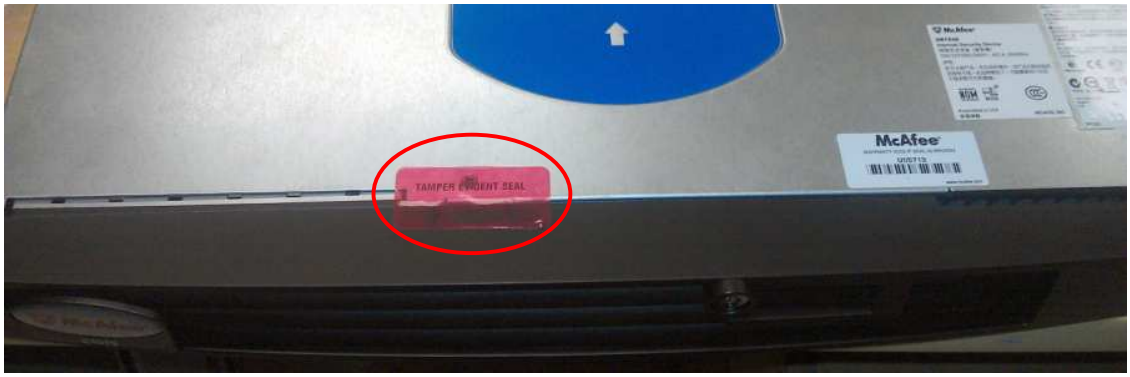

Figure 9 – C1015 Tamper-Evident Seal Placement (Top)

Figure 10 – C1015 Tamper-Evident Seal Placement (Bottom)

Figure 11, Figure 12 and Figure 13 show proper tamper-evident seal placement on the C2050 and C3000 Control Center.

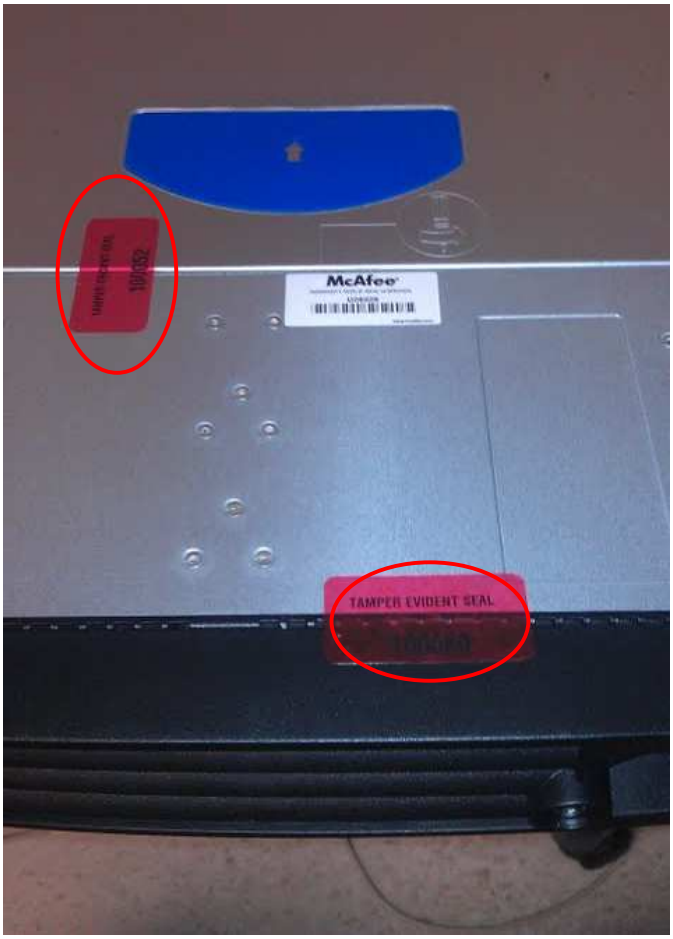

Figure 11 – C2050/C3000 Tamper-Evident Seal Placement (Top)

Figure 12 – C2050/C3000 Tamper-Evident Seal Placement (Bottom)

Figure 13 – C2050/C3000 Power Supply Tamper-Evident Seal Placement (Bottom)

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

Figure 14 shows the C1015 cryptographic module with the security baffles installed in the rear of the module.

Figure 14 – C1015 Security Baffle Placement

Figure 15 shows the C2050 cryptographic module with the security baffles installed in the rear of the module.

Figure 15 – C2050 Security Baffle Placement

Figure 16 shows the C3000 cryptographic module with the security baffles installed in the rear of the module.

Figure 16 – C3000 Security Baffle Placement

2.6 Operational Environment

The modules employ a non-modifiable operating environment, thus the operational environment requirements do not apply to the Firewall Enterprise Control Center.

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[15] – ECB[16], CBC[17], CFB[18](128), OFB[19](128): 128, 192 and 256 bit key sizes	1897
Triple-DES[20] – ECB, CBC, CFB(64), OFB(64): KO[21] 1, 2	1233
RSA ANSI[22] X9.31, PKCS[23]#1(v1.5, 2.1) Signature Generation/Verification – 1024, 1536 , 2048 , 3072 , 4096	972
RSA[24] ANSI X9.31 Key Generation – 1024, 1536, 2048, 3072, 4096	972
DSA[25] Key Generation – 1024	599
DSA PQG Generation/Verification – 1024	599
DSA Signature Generation/Verification – 1024	599
SHA[26]-1, SHA-224, SHA-256, SHA-384, SHA-512	1666

[15] AES – Advanced Encryption Standard
[16] ECB – Electronic Code Book
[17] CBC – Cipher Block Chaining
[18] CFB – Cipher Feedback
[19] OFB – Output Feedback
[20] DES – Data Encryption Standard
[21] KO – Keying Option
[22] ANSI – American National Standards Institute
[23] PKCS – Public-Key Cryptography Standards
[24] RSA – Rivest, Shamir, and Adleman
[25] DSA – Digital Signature Algorithm
[26] SHA – Secure Hash Algorithm

Algorithm	Certificate Number
HMAC[27]-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1137
SP[28] 800-38C based CCM[29]	1897
SP 800-38D based GCM[30]	1897
FIPS 186-2 PRNG	1009
SP800-90 HMAC DRBG[31]	163
SP800-90 Dual EC[32] DRBG	163

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	1831
Triple-DES – ECB, CBC, CFB(8), CFB(64), OFB: KO1,2	1184
DSA Key Generation: 1024-bit	575
DSA Signature Generation/Verification – Mod (1024)	575
RSA ANSI X9.31 Key Generation – 1024 to 4096-bit	920
RSA ANSI X9.31, PKCS #1.5, PSS sign/verify – 1024 to 4096-bit	920
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1611
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1085
ANSI X9.31 Appendix A.2.4 PRNG using AES	963

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

- Diffie-Hellman 1024 bits key (PKCS#3, key agreement/key establishment methodology provides 80 bits of encryption strength)
- RSA 1024-bit to 4096-bit key encrypt/decrypt (PKCS#1, key wrapping; key establishment methodology provides 80-150 bits of encryption strength)
- MD5[33] for hashing passwords

Additional information concerning SHA-1, Diffie-Hellman key agreement/key establishment, RSA key signatures, RSA key transport, two-key Triple-DES, ANSI X9.31 PRNG and specific guidance on

[27] HMAC – (keyed) Hash-based Message Authentication Code
[28] SP – Special Publication
[29] CCM – Counter with Cipher Block Chaining-Message Authentication Code
[30] GCM – Galois/Counter Mode
[31] DRBG – Deterministic Random Bit Generator
[32] EC – Elliptical Curve
[33] MD – Message Digest

transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The module supports the critical security parameters (CSPs) listed below in Table 9

Table 9 – 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-1024 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-1024 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-1	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
ANSI X9.31 PRNG seed	16 bytes of seed value	Generated internally by entropy gathering	Never leaves the module	Volatile memory in plain text	By power cycle or session termination	Used to generate FIPS approved random number
ANSI X9.31 PRNG key	AES 128 Key	Generated internally by entropy gathering	Never leaves the module	Volatile memory in plain text	By process termination	Used to generate FIPS approved random number
HMAC DRBG seed	Random Value	Generated internally by FIPS 186-2 PRNG	Never exits the module	Volatile memory in plain text	By power cycle	Used to seed the DRBG
HMAC DRBG key value	Random value	Generated internally by FIPS 186-2 PRNG	Never exits the module	Volatile memory in plain text	By process termination	Used in the process of generating a random number
HMAC DRBG V value	Random value	Generated internally by FIPS 186-2 PRNG	Never exits the module	Volatile memory in plain text	By process termination	Used in the process of generating a random number
EC DRBG seed	Random Value	Generated internally by FIPS 186-2 PRNG	Never exits the module	Volatile memory in plain text	By power cycle	Used to seed the DRBG
EC DRBG S value	Random value	Generated internally by FIPS 186-2 PRNG	Never exits the module	Volatile memory in plain text	By process termination	Used in the process of generating a random number

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
FIPS 186-2 PRNG Seed	Random value	Generated internally by entropy gathering	Never exits the module	Volatile Memory, in plain text	By power cycle or session termination	Used for generating random number for seeding approved DRBG
FIPS 186-2 PRNG Seed Key	Random value	Generated Internally by entropy gathering	Never exits the module	Volatile Memory, in plain text	By process termination	Used for generating random number for seeding approved DRBG
Integrity test key	HMAC SHA-1 key (Shared secret)	Hardcoded	Never exits the module	Volatile memory in plain text	Zeroized when the module firmware is reinstalled	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. To recover, the module must be reinstalled.

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

- Firmware integrity check (HMAC SHA-1)
- Approved Algorithm Tests
    - Crypto-J AES KAT[34]
    - OpenSSL AES 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-1 KAT
    - OpenSSL SHA-1 KAT
    - Crypto-J SHA-224 KAT
    - OpenSSL SHA-224 KAT
    - 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-1 KAT
    - OpenSSL HMAC SHA-1 KAT
    - Crypto-J HMAC SHA-224 KAT
    - OpenSSL HMAC SHA-224 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
    - SP800-90 Dual EC DRBG KAT
    - SP800-90 HMAC DRBG KAT
    - ANSI X9.31 RNG KAT
    - FIPS 186-2 PRNG KAT

[34] 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:

- ANSI X9.31 Continuous RNG
- FIPS 186-2 Continuous RNG
- Dual EC DRBG Continuous RNG
- HMAC DRBG Continuous RNG
- 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

2.8.3 Critical Functions Self-Tests

- SP800-90 Dual EC DRBG Instantiate Test
- SP800-90 Dual EC DRBG Reseed Test
- SP800-90 HMAC DRBG Instantiate Test
- SP800-90 HMAC DRBG Reseed Test

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 should be in charge of receiving, installing, initializing, and maintaining the Control Center. 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 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, the CO should 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
- Firewall Enterprise Control Center 5.x USB[35]
- McAfee Diagnostic USB
- 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

After unpacking the module and ensuring all materials are supplied, the CO should follow the included instructions for secure installation of the module into a rack system. Security baffles installation instructions are available as part of the FIPS Kit.

3.1.2 Initialization

There are two documents that should be used to initialize the Control Center for use on the network; *McAfee Firewall Enterprise Control Center: Quick Startup Guide* and *McAfee Firewall Enterprise Control Center: Product Guide*.

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 has the option of manually configuring the module directly on the appliance, or they can create a configuration file prior to powering up the appliance following the instructions in the guides listed above. The created configuration file can then be loaded at this time.

[35] USB – Universal Serial Bus

Once the Control Center has been fully configured, it will reboot and then give the option for the CO (*mgradmin* account) to login. When this prompt appears, the appliance has been properly configured and is ready to run in a non-FIPS-Approved mode of operation.

3.1.3 Configure FIPS settings

The Control Center is shipped and initially configured in a non-FIPS-Approved mode of operation. 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 to run in non-FIPS mode.

3.1.3.1 Configure the BIOS[36]

Once the module is securely installed and initialized, the CO must follow the instructions outlined in the *McAfee Firewall Enterprise Control Center 5.2.0 FIPS 140-2 Configuration Guide* and to *McAfee Firewall Enterprise Control Center Installation Guide FIPS 140-2 Level 2 Kit* to configure and password protect the BIOS. If the module is powered off, then power-up the system. Press the *<F2>* button when the McAfee logo appears. If the module is powered on, have the CO login in and type in the "*reboot"* command to reboot the appliance. The BIOS must be modified to ensure that the Control Center is only booted from the FIPS-enable hard drive, unauthorized users are unable to access the BIOS, and that the appliance will reset on AC Power Loss.

Once the BIOS has been configured, save all changes and exit. The appliance will reboot and the CO may continue to configure the module for FIPS-Approved mode.

3.1.3.2 Turning On FIPS Cryptography

The User must first 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 and FIPS self-tests will be run. More detailed instructions can be found in the *McAfee Firewall Enterprise Control Center 5.2.0 FIPS 140-2 Configuration Guide.*

The User will login to manage the Control Center via the Firewall Control Center Client Application with the appropriate username and password. Once logged in, the User will navigate to the "Control Center" tab at the top of the application. By double clicking the "FIPS" tree node and selecting "OK", both the Control Center and the Firewall Control Center Client Application will restart.

Once the Control Center has restarted and prompts for *mgradmin* login, the CO must configure the Control Center for FIPS Validated Mode. When in this mode, the Control Center is running in a FIPS-Approved mode of operation.

3.1.3.3 Enabling FIPS-Approved Mode

In FIPS Validated Mode, FIPS-Approved cryptographic libraries are used, keys comply with FIPS-Approved lengths, and FIPS self-tests are running. Root access and other OS-level account cannot login. The system's munix[37] mode of operation is disabled and only the *CO* has OS-level access (console and remote SSH). Instructions for enabling FIPS Validated Mode on the Control Center can be found in the *McAfee Firewall Enterprise Control Center 5.2.0 FIPS 140-2 Configuration Guide.*

The first thing the CO will do is replace all CSPs, certificates and SSH server keys. The CO will login using the *mgradmin* credentials that were set up during module initialization. Once logged in, the CO will login as root, and reboot the appliance. As soon as the module reboots and the splash screen appears, the

[36] BIOS – Basic Input Output System
[37] munix – system "maintenance kernel"

CO will force munix mode by pressing the "TAB" key repeatedly before the module can boot into normal operating conditions.

Once in munix mode, the CO will run two preconfigured scripts. The *fips_rmcerts* script will perform a set of commands that will remove server certificates and CSPs for FIPS-Approved use. The next script, *fips_block_munix*, will block access to the CLI when the system is in the munix mode of operation. Once this script is has completed, the system will restart back into server mode and prompt for *mgradmin* to login.

The last step to ensure the Control Center is running in a FIPS-Approved mode of operation is to block access to all OS-level accounts except for *mgradmin* (CO). At the login prompt, the CO will login then login once more as the *sso* user using the *su sso* command. As *sso*, the CO will run the script *fips_lock_accounts*, which will run a set of commands to block OS-level access to *root* and all other users. Once the script has finished, the CO will log out of *sso*, then reboot the module.

The module is now running in a FIPS-Approved mode of operation. To verify this, the CO may try to login as another user and may try to force the CLI in munix mode. The certificates must also be reestablished by the Firewall Control Center Client Application for remote firewall management.

3.1.4 Zeroization

After the Firewall Enterprise Control Center has been put into FIPS Validated 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 will then follow the steps outlined above to place the newly installed Control Center back into FIPS-Approved mode.

3.1.5 Installation of Secure Front Bezel

Access to the front panel of the Control Center modules may be required during initial set up; therefore, the front bezel should be installed last. The front bezel will prevent operators of the Control Center module from accessing the front USB port and power button of all devices as well as the DVD[38] drive and ID[39] button on the C2050 and C3000. To install the front bezel, you may refer to the guide included in the Control Center shipment materials. Access to the front panel of any of the modules should be limited to the CO.

3.1.6 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.
- 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

[38] DVD - Digital Video Disc
[39] ID - Identification

3.1.6.1 C1015 Tamper-Evident Seal Placement

Placement of the tamper-evident seals for the C1015 is shown in Figure 9 and Figure 10. Two tamper-evident seals will be used in total for this appliance. Figure 9 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 the placement of the sticker on 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 10 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.

3.1.6.2 C2050/C3000 Tamper-Evident Seal Placement

Placement of the tamper-evident seals for the C2050 and C3000 is shown in Figure 11, Figure 12 and Figure 13. The C2050 and C3000 will each require five tamper-evident seals. Figure 11 shows the seal placement on top of the appliance. There are two seals visible in Figure 11. The one farthest from the camera is placed between the removable top cover of the chassis and the main chassis. This ensures that any attempt to remove the top panel of the appliance will show evidence of tampering. The seal closest to the camera shows placement on both the chassis base and the front security bezel. Figure 13 shows the seal placement for removable power supplies.

Figure 12 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 popped off from either side of the chassis.

3.1.7 Module's Mode of Operation

After initial setup into FIPS mode, 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 FIPS-Approved mode or not.

Detailed steps and procedure required to determine whether the module is operating in FIPS-Approved mode or not can be found in the *McAfee Firewall Enterprise Control Center 5.2.0 FIPS 140-2 Configuration Guide*, which is available as a part of FIPS kit.

4 Acronyms

The Table 10 in this section defines the acronyms used in this document.

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input Output System
CA	Certificate Authority
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
CSEC	Communications Security Establishment Canada
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
EC	Elliptical Curve
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
ID	Identification
KAT	Known Answer Test
KO	Keying Option
LDAP	Lightweight Directory Access Protocol

Acronym	Definition
MD	Message Digest
Munix	System "maintenance kernel"
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
PRNG	Pseudo-Random Number Generator
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
RSBAC	Rule Set Based Access Control
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