McAfee, Inc.

Firewall Enterprise Control Center Virtual Appliance

Software Version: 5.3.2 Patch 6

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.13

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

1 INTRODUCTION 4
1.1 PURPOSE 4
1.2 REFERENCES 4
1.3 DOCUMENT ORGANIZATION 4
2 CONTROL CENTER 5
2.1 OVERVIEW 5
2.1.1 Control Center Architecture Overview 5
2.2 MODULE SPECIFICATION 7
2.2.1 Physical Cryptographic Boundary 7
2.2.2 Logical Cryptographic Boundary 8
2.3 MODULE INTERFACES 9
2.4 ROLES AND SERVICES 10
2.4.1 Crypto Officer Role 10
2.4.2 User Role 11
2.4.3 Non-Security Relevant Services 12
2.4.4 Authentication 12
2.5 PHYSICAL SECURITY 13
2.6 OPERATIONAL ENVIRONMENT 13
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 13
2.8 SELF-TESTS 20
2.8.1 Power-Up Self-Tests 20
2.8.2 Conditional Self-Tests 20
2.9 MITIGATION OF OTHER ATTACKS 21
3 SECURE OPERATION 22
3.1 CO AND USER GUIDANCE 22
3.1.1 Initial Setup 22
3.1.2 Initialization 22
3.1.3 Configure FIPS settings 22
3.1.4 Password Management 23
3.1.5 Module's Mode of Operation 23
3.1.6 Zeroization 23
4 ACRONYMS 24

Table of Figures

FIGURE 1 – CONTROL CENTER VIRTUAL APPLIANCE ARCHITECTURE 6
FIGURE 2 – GPC BLOCK DIAGRAM 8
FIGURE 3 – CONTROL CENTER LOGICAL CRYPTOGRAPHIC BOUNDARY 9

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION 6
TABLE 2 – FIPS 140-2 LOGICAL INTERFACE MAPPINGS 9
TABLE 3 – CO SERVICES 10
TABLE 4 – USER SERVICES 11
TABLE 5 – AUTHENTICATION MECHANISM STRENGTHS 13
TABLE 6 – CRYPTO-J FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 13
TABLE 7 – OPENSSL FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 14
TABLE 8 – NETWORK PROTOCOL COMPONENT VALIDATION 15
TABLE 9 – LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 16

TABLE 10 – ACRONYMS 24

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Firewall Enterprise Control Center Virtual Appliance from McAfee, Inc. This Security Policy describes how the Firewall Enterprise Control Center Virtual Appliance 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 1 FIPS 140-2 validation of the module. The Firewall Enterprise Control Center Virtual Appliance is referred to in this document as the Control Center, the MFECC, the virtual appliance, the 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 Control Center

2.1 Overview

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. This capability provides a high level overview of network activity and behavior, which can be drilled down 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).

The Virtual Appliance is just one offering of a line of McAfee Firewall Enterprise Control Center appliances. McAfee offers three more Control Center appliances, which are hardware appliances in a 1U rack mountable chassis form factor. The hardware appliances are FWE-C1015, FWE-C2050, and FWE-C3000. A separate Security Policy for the hardware appliances can be found on the CMVP website.

2.1.1 Control Center Architecture Overview

The Control Center Server software is written in both C++ and Java, and compiled to run on McAfee's own McAfee Linux Operating System (MLOS) v2.2.3. The software 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 GUI.
- Tomcat – It is used to facilitate communication between the Control Center server and its client application or firewalls within its scope of control.
- Database – A PostgreSQL database is used to store policy and configuration data.
- DCS[2] – It 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.
- Control Center Features – It consists of the code behind the management functionality provided to the GUI including Control Center Server and firewall backup and restore operations, provisioning of configuration domains and HA[4] topologies, software updates, the ePolicy Orchestrator extension, and the security event manager.

[1] GUI – Graphical User Interface

[2] DCS – Data Collection Server

[3] UTT – User Datagram Protocol (UDP) over Transmission Control Protocol (TCP) Tunnel

[4] HA – High Availability

Figure 1 shows the basic architecture of a Control Center Virtual Appliance deployment. The dotted lines indicate the logical cryptographic boundary (red) and physical cryptographic boundary (green) of the module.

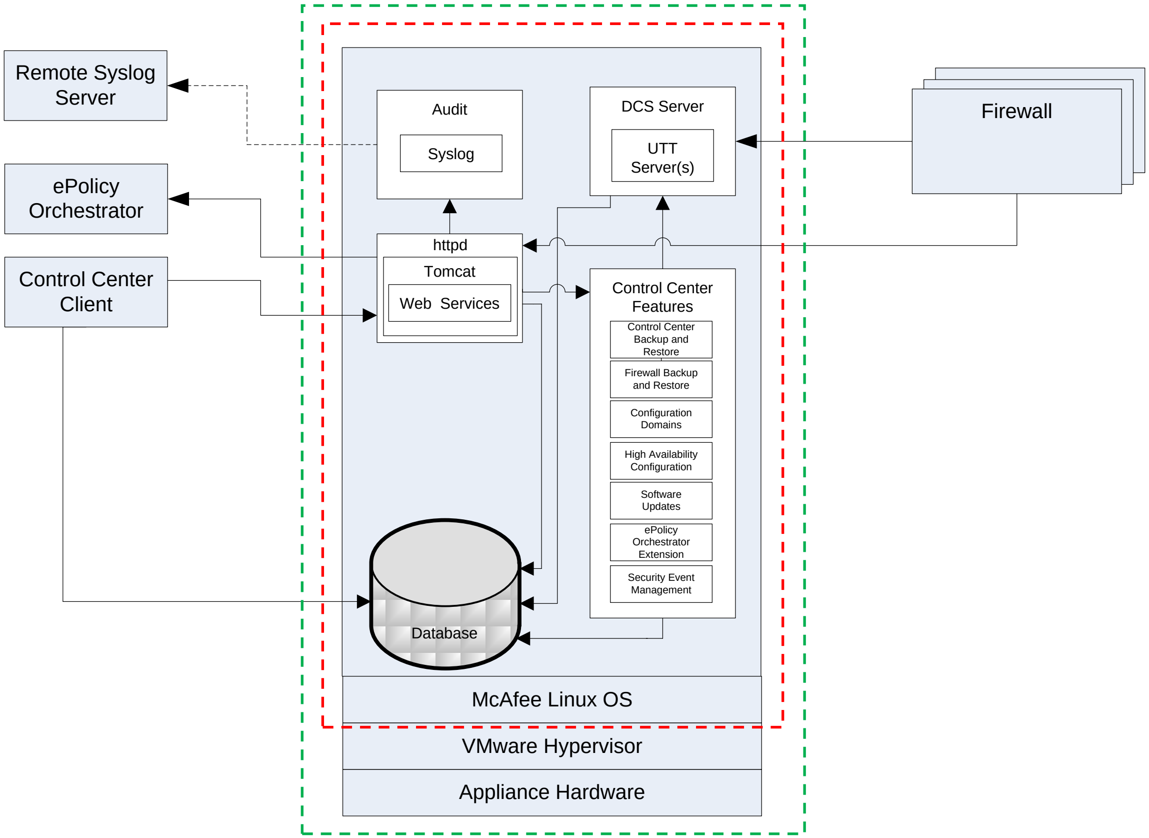


Figure 1 – Control Center Virtual Appliance Architecture[5]

The Control Center is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[6]	1

[5] httpd – hyper-text transfer protocol (HTTP) daemon

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

.

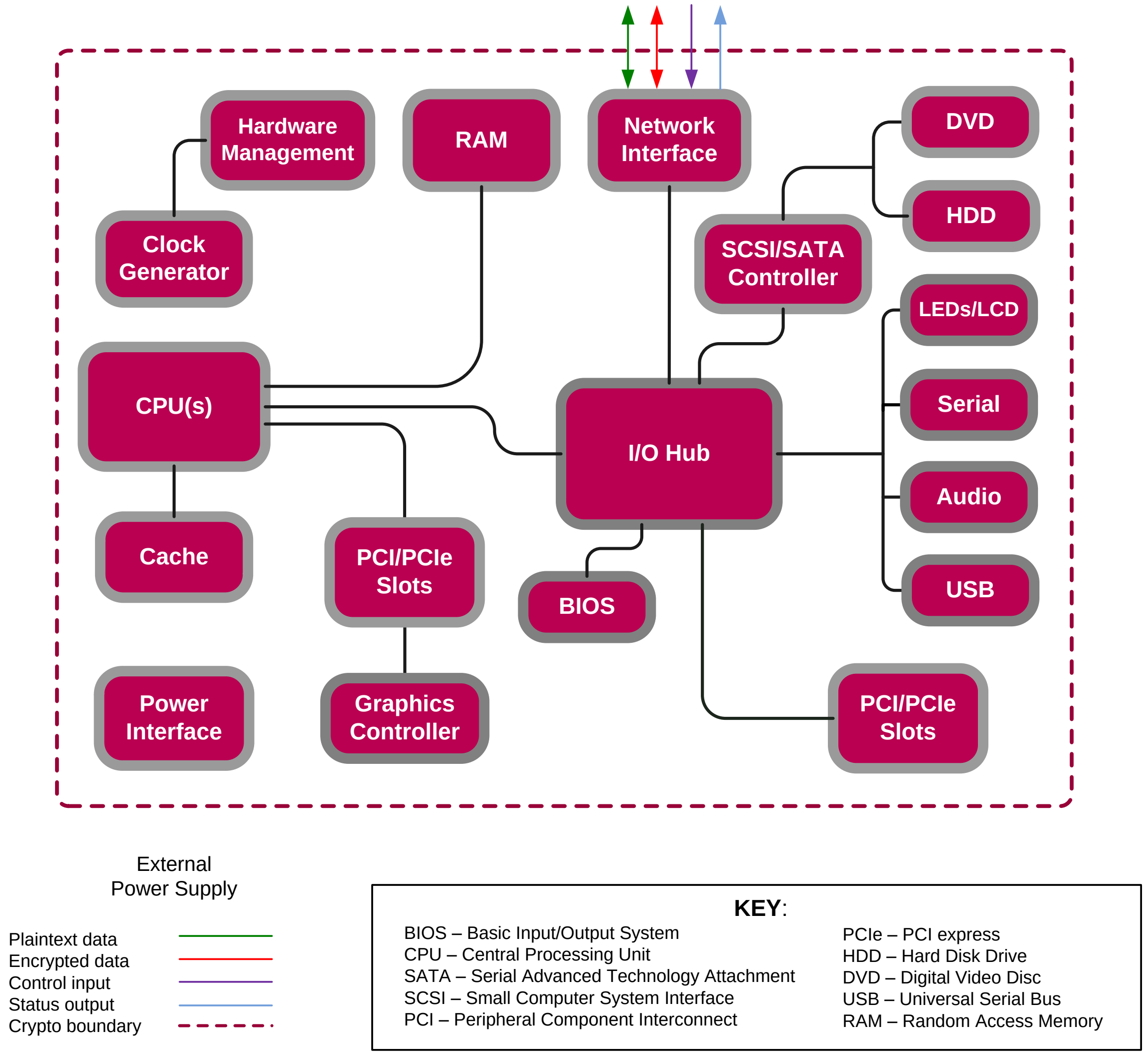
Section	Section Title	Level
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Control Center is a software module (Software Version: 5.3.2 Patch 6) with a multi-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary of the module consists of the Control Center application software, two cryptographic libraries and MLOS v2.2.3 as shown by the red-colored dotted line in Figure 1. The Firewall Enterprise Control Center Virtual Appliance was tested as meeting Level 1 FIPS compliance with MLOS v2.2.3. on VMware vSphere 5.0 hypervisor running on a Intel SR2625URLX. McAfee affirms the module will operate in its FIPS-Approved configuration on a general purpose computing device running MLOS v2.2.3 and VMware vSphere 5.0.

2.2.1 Physical Cryptographic Boundary

As a software cryptographic module, there are no physical protection mechanisms implemented. Therefore, the module must rely on the physical characteristics of the host system. The physical boundary of the cryptographic module, running within a virtual environment, is defined by the hard enclosure around the host system on which it runs, as shown by the green-colored dotted line in Figure 1. The module supports the physical interfaces of a General Purpose Computer (GPC) which directly hosts the virtual environment the module has been installed on. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM, hard disk, device case, power supply, and fans. See Figure 2 for a block diagram of a GPC hardware appliance.



KEY:

BIOS – Basic Input/Output System
CPU – Central Processing Unit
SATA – Serial Advanced Technology Attachment
SCSI – Small Computer System Interface
PCI – Peripheral Component Interconnect
PCIe – PCI express
HDD – Hard Disk Drive
DVD – Digital Video Disc
USB – Universal Serial Bus
RAM – Random Access Memory

Figure 2 – GPC Block Diagram

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the module consists of two cryptographic libraries and the Control Center application software compiled to run on MLOS v2.2.3. Figure 1 and Figure 3 show logical block diagrams of the module executing in memory and its interactions with the VMware vSphere hypervisor through the module's defined logical cryptographic boundary. The module interacts directly with the hypervisor, which runs directly on the GPC, as defined in Section 2.2.1 above. The hypervisor controls and directs all interactions between the Control Center and the operator.

.

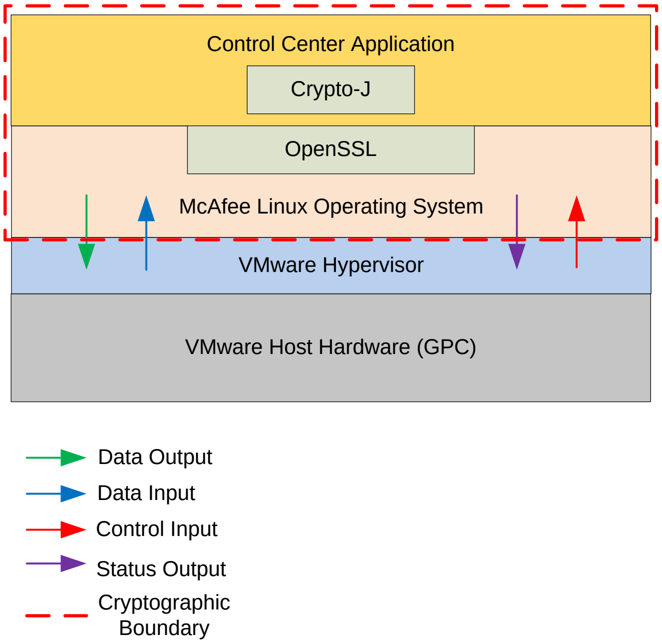


Figure 3 – Control Center Logical Cryptographic Boundary

2.3 Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output

As a software module, the virtual appliance has no physical characteristics. The module's physical and electrical characteristics, manual controls, and physical indicators are those of the host system. The VMware hypervisor provides virtualized ports and interfaces for the module. Interaction of with the virtual ports created by the hypervisor occurs through the host system's Ethernet port. Management, data, and status traffic must all flow through the Ethernet port. Direct interaction with the module via the host system is not possible. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 2 below.

Table 2 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Logical Port/Interface	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet Ports, Virtual USB Ports, Virtual Serial Ports	• Data Input • Data Output • Control Input • Status Output

Data input and output are the packets utilizing the services provided by the modules. These packets enter and exit the module through the Virtual Ethernet ports. Control input consists of Configuration or Administrative data entered into the modules. Status output consists of the status provided or displayed via the user interfaces (such as GUI or CLI) or available log information.

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 (CO) 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 CO 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 3 below.

Table 3 – 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[7] Public/Private Key – W Web Server Public/Private Key – W PostgreSQL Public/Private Key – W DCS Public/Private Key – W SSH[8] 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

[7] CA – Certificate Authority

[8] SSH – Secure Shell

Service	Description	Input	Output	Approved Algorithms Accessed	CSP and Type of Access
Access CLI[9] Services[10]	Access the CLI over Host system Ethernet ports or Host system 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 GUI. 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 4 below.

Table 4 – 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 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

[9] CLI – Command Line Interface
[10] The SSH protocol has not been reviewed or tested by the CAVP or CMVP
[11] RADIUS – Remote Authentication Dial In User Service
[12] LDAP – Lightweight Directory Access Protocol

.

Service	Description	Input	Output	Approved Algorithms Accessed	CSP and Type of Access
Show Status	Show status of the module	Command and parameters	Command response and status output	N/A	None
Access GUI[13] services[14]	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 Key – X Web Server Private Key – X Web Server Session Key – W, X PostgreSQL Public Key – X PostgreSQL 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 Virtual Appliance 5.3.2 Product Guide; Revision A (2013)*. The product guide is freely available at http://www.mcafee.com/us/downloads/downloads.aspx.

2.4.4 Authentication

The Control Center Virtual Appliance supports 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 of this document. Once the operator is authenticated, they will assume their respective role and carry out the available services listed in Table 3 and Table 4. All users authenticate to the module using User-ID and passwords.

2.4.4.1 Authentication Data Protection[15]

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[16] hash function and stores the hashed password in a password database.

2.4.4.2 Authentication Mechanism Strength

Please refer to Table 5 for information on authentication mechanism strength:

[13] GUI – Graphical User Interface

[14] The Transport Layer Security (TLS) protocol has not been reviewed or tested by the CAVP or CMVP

[15] "Protection" does not imply cryptographic protection

[16] MD5 – Message Digest 5

.

Table 5 – Authentication Mechanism Strengths

Role	Type of Authentication	Authentication Strength
CO 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 ($1000\text{x}10^6$ × 60 = $6\text{x}10^{10}$ =) 60,000,000,000 bits of data can be transmitted in one minute. Each password is 64 bits, meaning $9.375\text{x}10^8$ 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

Firewall Enterprise Control Center Virtual Appliance is a software module, which FIPS defines as a multi-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The operational environment for the module consists of MLOS v2.2.3 and the VMware hypervisor. The module was tested and found to be compliant with FIPS 140-2 Level 1 requirements on an Intel SR2625URLX hardware appliance running MLOS v2.2.3 and VMware vSphere 5.0. All cryptographic keys and CSPs are under the control of MLOS and the hypervisor, which protect the CSPs against unauthorized disclosure, modification, and substitution. McAfee affirms the module will operate in its FIPS-Approved configuration on any general purpose computing device running MLOS v2.2.3 and VMware vSphere 5.0.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 6 and Table 7 below.

Table 6 – Crypto-J FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES[17] – ECB[18], CBC[19], CFB[20](128), OFB[21]: 128, 192 and 256 bit key sizes	2973

[17] AES – Advanced Encryption Standard

[18] ECB – Electronic Code Book

Algorithm	Certificate Number
Triple-DES[22] – ECB, CBC, CFB(64), OFB: KO[23] 1	1762
RSA ANSI[24] X9.31, PKCS[25]#1(v1.5, 2.1) Signature Generation/Verification – 2048- and 3072-bit	1562
RSA ANSI X9.31 Key Generation –2048- and 3072-bit	1562
DSA Key Generation signature – 2048-bit	886
DSA PQG Parameter Generation/Verification – 2048 bit	886
DSA Signature Generation/Verification – 2048-bit	886
SHA[26]-256, SHA-384, SHA-512	2499
HMAC[27] SHA-256, HMAC SHA-384, HMAC SHA-512	1885
SP[28] 800-38C based CCM[29]	2973
SP 800-38D based GCM[30]	2973
SP800-90A HMAC DRBG	567

Table 7 – OpenSSL FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES – ECB, CBC, CFB(8), CFB(128), OFB, : 128, 192, and 256 bit key sizes	3117
Triple-DES – ECB, CBC, CFB(8), CFB(64), OFB: KO1	1788
DSA Key Generation: 2048-bit	901
DSA Signature Generation/Verification : 2048 bit	901
RSA FIPS 186-4 Key Generation: 2048- and 3072-bit	1588
RSA (FIPS 186-4) ANSI X9.31, PKCS #1.5, PSS signature generation – 2048- and 3072-bit	1588
RSA (FIPS 186-4) ANSI X9.31, PKCS #1.5, PSS signature verification – 1024-, 2048-, and 3072-bit	1588
RSA (FIPS 186-2) ANSI X9.31, PKCS #1.5, PSS signature verification – 1024-, 2048-, 3072-, and 4096-bit	1588

[19] CBC – Cipher Block Chaining
[20] CFB – Cipher Feedback
[21] OFB – Output Feedback
[22] DES – Data Encryption Standard
[23] KO – Keying Option
[24] ANSI – American National Standards Institute
[25] PKCS – Public-Key Cryptography Standards
[26] SHA – Secure Hash Algorithm
[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

Algorithm	Certificate Number
SHA-256, SHA-384, SHA-512	2573
HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	1954
SP800-90A HASH DRBG	628

The cryptographic module implements the TLS[31] 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 8. The complete protocol implementations have not been reviewed or tested by the CAVP[32] and CMVP.

Table 8 – Network Protocol Component Validation

Algorithm	CVL Certificate Number
TLS[33] 1.0/1.1 and TLS 1.2 KDF using SHA 256 and SHA 384	379
SSH KDF using SHA-256, -384, and -512	379

The module utilizes the following non-compliant algorithm implementation, which is 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 6 and Table 7.

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementation 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 for hashing passwords; creating SCEP[34] fingerprint

Caveat: Additional information concerning 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.

[31] TLS – Transport Layer Security
[32] CAVP – Cryptographic Algorithm Validation Program
[33] TLS – Transport Layer Security
[34] SCEP – Simple Certificate Enrollment Protocol

.

The module supports the critical security parameters (CSPs) listed 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 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 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 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 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 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 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 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 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 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 is reinstalled	It is used by the SSH server to authenticate itself for incoming connections
SSH Private Key	RSA-2048 or DSA-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 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 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 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 is reinstalled	Used for authenticating all COs (over CLI) and Users (over GUI)
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 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

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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 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 software integrity test

.

2.8 Self-Tests

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

2.8.1 Power-Up Self-Tests

Power-Up Self-Tests are performed 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 it 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 software with the supplied materials.

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

- Software integrity check (HMAC SHA-256)
- Approved Algorithm Tests
  - Crypto-J AES Encrypt KAT[35]
  - 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 SP800-90A HMAC DRBG KAT
  - OpenSSL SP800-90A HASH DRBG KAT

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

[35] KAT – Known Answer Test

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 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
- Software upgrade test using 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 1 requirements for this validation.

3 Secure Operation

The Control Center meets Level 1 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. 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.

Caveat: This guide assumes that a virtual environment is already setup and it is ready to accept a new virtual machine.

3.1.1 Initial Setup

The Control Center module is be shipped as an ISO[36] file to be installed on a preconfigured virtual environment (see requirements below). Install the Control Center software by following the steps outlined in the ”Install Control Center software” section of the *McAfee Firewall Enterprise Control Center 5.3.2 FIPS 140-2 Configuraiton Guide*. Control Center shall be installed using the VMware vSphere 5.0 desktop client. The virtual environment shall be set up to meet the following minimum specifications:

- 2048 MB memory
- 1 CPU
- 2 Network adapters
- 1 Hard Disk

Once the virtual machine has been installed onto the host, start up the Control Center software and prepare for initialization

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-Approved mode, the module must be reinstalled to restore the original factory configuration.

[36] ISO – International Organizatoin for Standardization

.

3.1.3.1 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 and FIPS self-tests will be run. 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.*

3.1.3.2 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 account cannot login after the FIPS-Approved mode is enabled. Detailed instructions for enabling FIPS-Approved 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).

3.1.3.3 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.

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

4 Acronyms

Table 10 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
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
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
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
ISO	International Organizatoin for Standardization
KAT	Known Answer Test
KDF	Key Derivation Function
KO	Keying Option
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5

.

Acronym	Definition
MLOS	McAfee Linux Operating System
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PKCS	Public-Key Cryptography Standards
RADIUS	Remote Authentication Dial-In User Service
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
TLS	Transport Layer Security
UTT	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