McAfee, Inc.

Firewall Enterprise Control Center Virtual Appliance

Software Version: 5.2.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.2

Prepared for:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Firewall Enterprise Control Center 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 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 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 C1015, C2050, and C3000.

2.1.1 Control Center Architecture Overview

The Control Center Server software is written in both C++ and Java, and compiled to run on CGLinux secured by McAfee with RSBAC[2], an open-source access control framework. 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[3] – It 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.
- 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[5] topologies, software updates, the ePolicy Orchestrator extension, and the security event manager.

[1] GUI – Graphical User Interface
[2] RSBAC – Rule Set Based Access Control
[3] DCS – Data Collection Server
[4] UTT – User Datagram Protocol (UDP) over Transmission Control Protocol (TCP) Tunnel
[5] HA – High Availability

Figure 1 shows the basic architecture of a Control Center Virtual Appliance deployment. The dotted lines indicate the cryptographic and physical boundaries of the module.

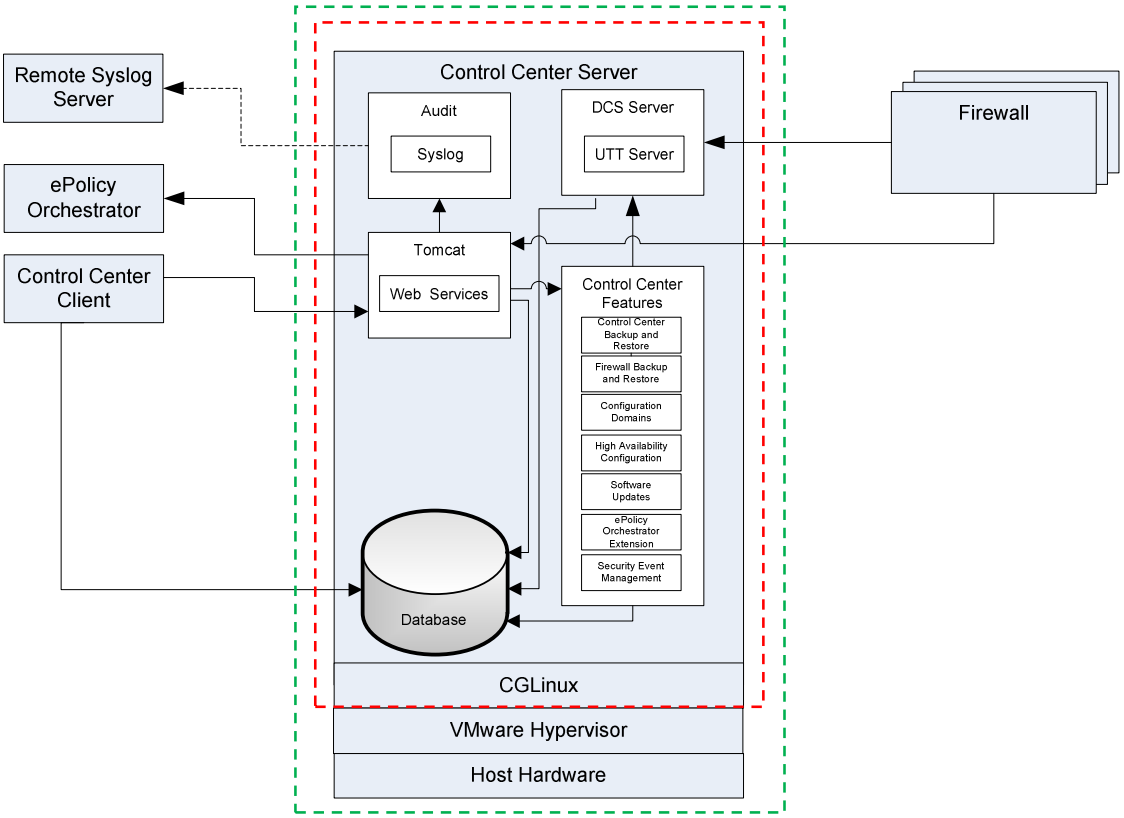

Figure 1 - Control Center Virtual Appliance Architecture

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
9	Self-tests	1

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

Section	Section Title	Level
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Control Center is a software module (Software Version Software Version: 5.2.0) with a multi-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary of the module Control Centerconsists of Control Center application software, two cryptographic libraries and a modified version of CGLinux as shown by the red-colored dotted line in Figure 1. It is designed to execute on a host system running VMware hypervisor on a General Purpose Computer (GPC) hardware platform. As a virtual appliance, the Control Center must be installed on a supported virtual machine hypervisor. The module was tested and found compliant on VMware vSphere 4.1 hypervisor.

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 GPC which can directly host 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 standard GPC block diagram.

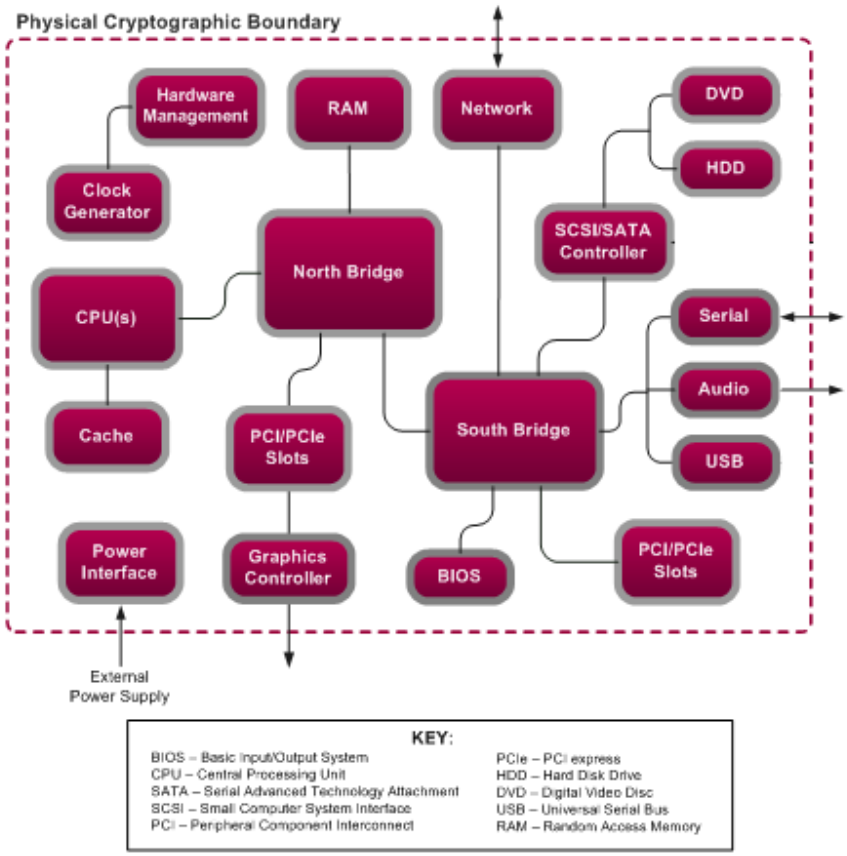

Figure 2 - GPC Block Diagram

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 a modified version of CGLinux. Figure 1 and Figure 3 show a logical block diagram 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 a GPC as defined in Section 2.2.1 above. The hypervisor controls and directs all interactions between the Control Center and the operator.

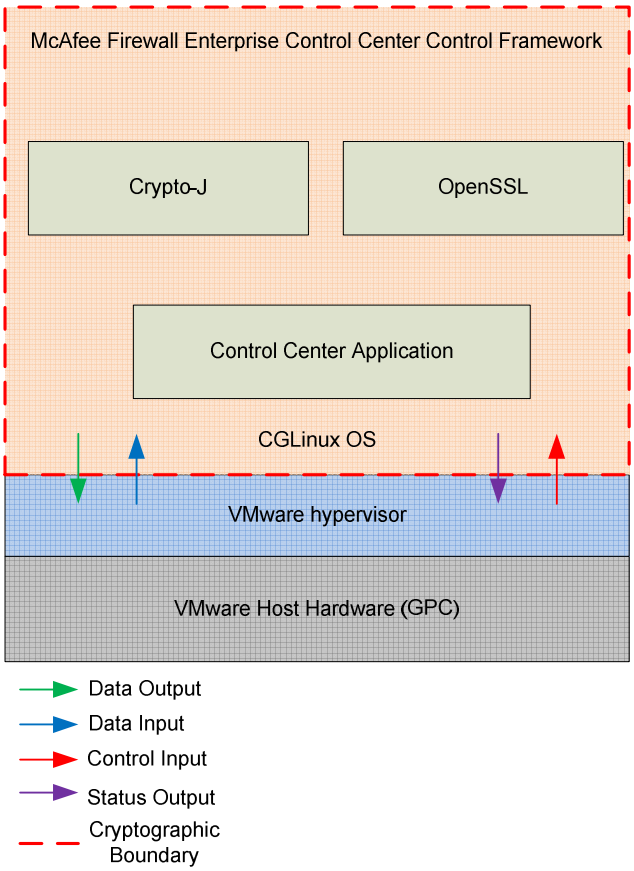

Figure 3 - Control Center Logical Cryptographic Boundary

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. 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	• Data Input • Data Output • Control Input • Status Output
Host System Keyboard port	Virtual Keyboard port	• Control Input
Host System Mouse port	Virtual Mouse port	• Control Input
Host System Serial Port	Virtual Serial Port	• Data Input • Control Input
Host System Video Connector	Virtual Video Interface	• Status Output
Host System Power Interface	N/A	• Power

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	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[7] 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[8] Services	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	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[9] and LDAP[10] 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	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

[7] CA – Certificate Authority
[8] CLI – Command Line Interface
[9] RADIUS – Remote Authentication Dial In User Service
[10] LDAP – Lightweight Directory Access Protocol

Service	Description	Input	Output	CSP and Type of Access
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[11] 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 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 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.

[11] GUI – Graphical User Interface

2.4.3.1 Authentication Data Protection[12]

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 MD[13]5 hash function and stores the hashed password in a password database.

2.4.3.2 Authentication Mechanism Strength

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

Table 5 - Authentication Mechanism Strengths

Role	Type of Authentication	Authentication Strength
CO 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 1 in 100,000 as required by FIPS 140-2.

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 CGLinux and the VMware hypervisor. The module was tested and found to be compliant with FIPS 140-2 requirements on VMware vSphere 4.1 hypervisor running on a standard GPC configuration. All cryptographic keys and CSPs are under the control of the CGLinux operating system and the hypervisor, which protect the CSPs against unauthorized disclosure, modification, and substitution.

[12] "Protection" does not imply cryptographic protection
[13] MD – Message Digest

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[14] – ECB[15], CBC[16], CFB[17](128), OFB[18] (128): 128, 192 and 256 bit key sizes	1917
Triple-DES[19] – ECB, CBC, CFB(64), OFB(64): KO[20] 1, 2	1247
RSA ANSI[21] X9.31, PKCS[22]#1(v1.5, 2.1) Signature Generation/Verification – 1024, 1536 , 2048 , 3072 , 4096	985
RSA ANSI X9.31 Key Generation – 1024, 1536, 2048, 3072, 4096	985
DSA Key Generation signature – 1024	608
DSA PQG parameters Generation/Verification – 1024	608
DSA Signature Generation/Verification – 1024	608
SHA[23]-1, SHA-224, SHA-256, SHA-384, SHA-512	1683
HMAC[24]-SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC-SHA-384, HMAC SHA-512	1152
SP[25] 800-38C based CCM[26]	1917
SP 800-38D based GCM[27]	1917
FIPS 186-2 PRNG	1008
SP800-90 HMAC DRBG[28]	162
SP800-90 Dual EC[29] DRBG	162

[14] AES – Advanced Encryption Standard
[15] ECB – Electronic Code Book
[16] CBC – Cipher Block Chaining
[17] CFB – Cipher Feedback
[18] OFB – Output Feedback
[19] DES – Data Encryption Standard
[20] KO – Keying Option
[21] ANSI – American National Standards Institute
[22] PKCS – Public-Key Cryptography Standards
[23] SHA – Secure Hash Algorithm
[24] HMAC – (keyed) Hash-based Message Authentication Code
[25] SP – Special Publication
[26] CCM – Counter with Cipher Block Chaining-Message Authentication Code
[27] GCM – Galois/Counter Mode
[28] DRBG – Deterministic Random Bit Generator
[29] EC – Elliptical Curve

Table 7 - OpenSSL MFE FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES – ECB, CBC, CFB(8), CFB(128), OFB, : 128, 192, and 256 bit key sizes	1862
Triple-DES – ECB, CBC, CFB(8), CFB(64), OFB: KO1, 2	1209
DSA Key Generation: 1024-bit keys	581
DSA Signature Generation/Verification : 1024 bit keys	581
RSA ANSI X9.31 Key Generation: 1024- to 4096-bit keys	943
RSA ANSI X9.31, PKCS #1.5, PSS sign/verify – 1024 to 4096-bit keys	943
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1638
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC-SHA-384, HMAC SHA-512	1109
ANSI X9.31 Appendix A.2.4 PRNG[30] using AES	976

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

[30] PRNG – Pseudo-Random Number Generator

The module supports the critical security parameters (CSPs) listed in Table 8.

Table 8 - 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-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 is reinstalled	It is used by the SSH server to authenticate itself for incoming connections
SSH Private Key	RSA-2048 or DSA-1024 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-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 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
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
FIPS 186-2 PRNG Seed	Random value	Generated internally	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	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 is reinstalled	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. To recover, the module must be reinstalled.

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

- Software integrity check (HMAC SHA-1)
- Approved Algorithm Tests
    - Crypto-J AES KAT
    - 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

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 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 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 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.

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

3.1.1 Initial Setup

The Control Center will be shipped as a .vmdk[31] file with preset configurations for the virtual environment. Install the .vmdk file by following the steps outlined in the *MFECC Virtual Appliance Installation Guide.* Control Center will be installed using the VMware vSphere 4.1 desktop client. The virtual machine is set up to meet the following minimum specifications:

- 1024 MB memory
- 1 CPU
- 2 Network adapters
- 1 Hard Disk (size varies based on GPC configuration)

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

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 5.2.0 FIPS 140-2 Configuration Guide* and *MFECC 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 virtual appliance, or they can create a configuration file prior to powering up the virtual appliance following the instructions in the guides listed above. The created configuration file can then be loaded at this time.

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 mode 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.

[31] VMDK – Virtual Machine Disk Format

NOTE: This is a one-way operation. Once the module has been configured for FIPS-Approved mode, the module must be completely reset and reinstalled to run in non FIPS-Approved mode.

3.1.3.1 Turning On FIPS Cryptography

The User must first enable FIPS cryptography through the GUI. Turning on FIPS cryptography means that the system will use FIPS-Approved cryptographic libraries and keys. 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 GUI with the appropriate username and password. Once logged in, the User will navigate to the "Control Center" tab at the header part of the GUI window. By double clicking the "FIPS" tree node and selecting "OK", both the Control Center and the GUI 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.

3.1.3.2 Enabling FIPS Validated 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. USB ports are disabled from being mounted for use. The system's munix[32] 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 shall perform is to replace all CSPs, certificates and SSH server keys. The CO will login using the *mgradmin* credentials that were set up during module initialization. The CO will re-authenticate as a root user, and reboot the appliance. As soon as the module reboots and the splash screen appears, the 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 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 as *mgradmin* then execute the command "*su sso*" to login under the *sso* user account. 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 as user *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 GUI for remote firewall management.

3.1.4 Zeroization

After the 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 completed. The CO will then follow the steps outlined above to place the newly installed Control Center back into FIPS validated mode.

[32] munix – system "maintenance kernel"

3.1.5 Module's Mode of Operation

After initial setup into FIPS mode, the module can only be operated in the FIPS-Approved mode of operation. The CO or any authorized User can access the module via the GUI 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*.

4 Acronyms

The Table 9 in this section defines the acronyms used in this document.

Table 9 - 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
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
EC	Elliptical Curve
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GPC	General Purpose Computer
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash Message Authentication Code
KAT	Known Answer Test
KO	Keying Option
LDAP	Lightweight Directory Access Protocol
MD	Message Digest
Munix	System “maintenance kernel”

Acronym	Definition
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PKCS	Public-Key Cryptography Standards
PRNG	Pseudo-Random Number Generator
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
VMDK	Virtual Machine Disk Format

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