McAfee, Inc.

McAfee Firewall Enterprise Virtual Appliance for Crossbeam

Software Version: 8.3.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.0

Prepared for:

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, California 95054
United States of America

Phone: +1 408 988 3832
http://www.mcafee.com

Prepared by:

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

Phone: +1 703 267 6050
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 McAfee Firewall Enterprise Virtual Appliance for Crossbeam from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise Virtual Appliance for Crossbeam (Software Version: 8.3.1) 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 McAfee Firewall Enterprise Virtual Appliance for Crossbeam is referred to in this document as the MFE for Crossbeam, the cryptographic 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 corporate 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
- Validation Submission Summary 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 MFE for Crossbeam

2.1 Overview

McAfee, Inc. is a global leader in Enterprise Security solutions. The company's comprehensive portfolio of network security products and solutions provides unmatched protection for the enterprise in the most mission-critical and sensitive environments. McAfee's Firewall Enterprise solutions were created to meet the specific needs of organizations of all types and enable those organizations to reduce costs and mitigate the evolving risks that threaten today's networks and applications.

Consolidating all major perimeter security functions into one system, the McAfee Firewall Enterprise appliances are the strongest self-defending perimeter firewalls in the world. Built with a comprehensive combination of high-speed application proxies, reputation-based threat intelligence, and signature-based security services, Firewall Enterprise defends networks and Internet-facing applications from all types of malicious threats, both known and unknown.

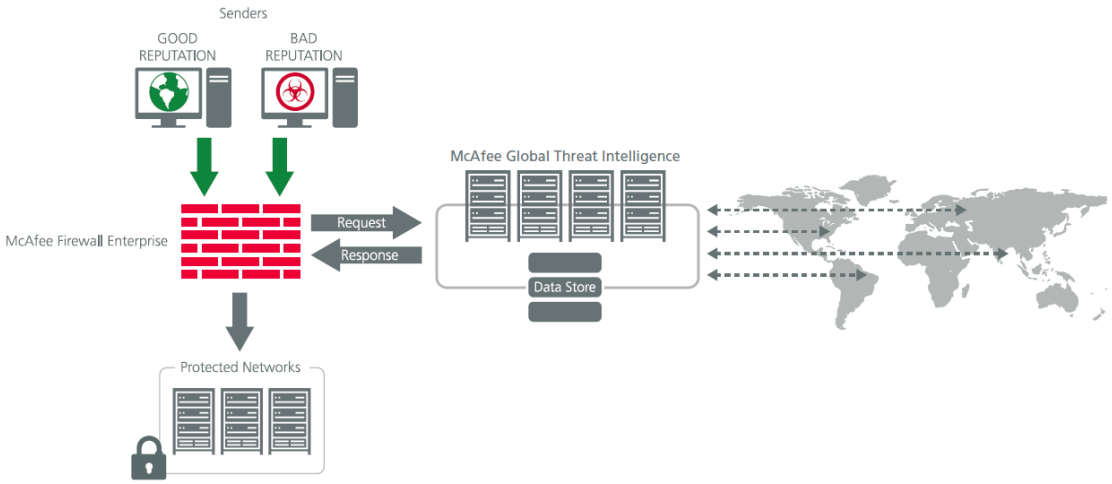

Figure 1 – Typical Deployment Scenario

Firewall Enterprise appliances are market-leading, next-generation firewalls that provide application visibility and control even beyond Unified Threat Management (UTM) for multi-layer security – and the highest network performance. Global visibility of dynamic threats is the centerpiece of Firewall Enterprise and one of the key reasons for its superior ability to detect unknown threats along with the known. Firewall Enterprise appliances deliver the best-of-breed in security systems to block attacks, including:

- Viruses
- Worms
- Trojans
- Intrusion attempts
- Spam and phishing tactics
- Cross-site scripting
- Structured Query Language (SQL) injections
- Denial of service (DoS)
- Attacks hiding in encrypted protocols

Firewall Enterprise security features include:

- Firewall feature for full application filtering, web application filtering, and Network Address Translation (NAT)
- Authentication using local database, Active Directory, LDAP[1], RADIUS[2], Windows Domain Authentication, and more
- High Availability (HA)
- Geo-location filtering
- Encrypted application filtering using TLS[3] and IPsec[4] protocols
- Intrusion Prevention System
- Networking and Routing
- Management via Simple Network Management Protocol (SNMP) version 3
- Per-connection auditing and policy enforcement of endpoints via DTLS[5] protocol

The McAfee Firewall Enterprise Virtual Appliance for Crossbeam is designed to leverage Crossbeam's X-Series Operating System (XOS) virtualization features and run as a virtual appliance. It is intended to run on a Crossbeam Application Processor Module (APM) blade installed in a Crossbeam X-Series chassis.

The MFE for Crossbeam can be managed locally or remotely using one of three available management tools:

- MFE Control Center – Control Center is an enterprise-class management appliance that 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. Control Center is designed to run on an administrator's workstation, and allows network administrators to fully mange their firewall solutions from the network edge to the core. Management communications between the MFE and Control Center are secured over a TLS session.

  For more information regarding Control Center, please refer to McAfee's Control Center product documentation.

- Command Line Interface (CLI) – A UNIX-based CLI is also available for configuring the firewall and performing troubleshooting tasks. The CLI is accessed locally over the serial port or by a direct-connected keyboard and mouse, while remote access is via Secure Shell (SSH) session.

- SNMP v3 – The MFE for Crossbeam uses the SNMP v3 protocol for remote management, and to provide information about the state and statistics as part of a Network Management System (NMS). Although SNMP v3 can support AES encryption, the protocol employs a non-Approved key generation method; therefore, the module has been designed to block the ability to view or alter critical security parameters (CSPs) through this interface. This is a management-only interface for the module; no CSPs or user data are transmitted over this interface.

The McAfee Firewall Enterprise Virtual Appliance for Crossbeam is validated at the 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	3

[1] LDAP – Lightweight Directory Access Protocol
[2] RADIUS – Remote Authentication Dial-In User Service
[3] TLS – Transport Layer Security
[4] IPsec – Internet Protocol Security
[5] DTLS – Datagram Transport Layer Security

Section	Section Title	Level
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
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The McAfee Firewall Enterprise Virtual Appliance for Crossbeam is a multi-chip standalone software module that meets overall Level 1 FIPS 140-2 requirements. It executes as a virtual appliance, running on a proprietary guest operating system (OS) in a virtualized environment on a purpose-built computing platform.

The guest operating system is McAfee's SecureOS v8.3, while the virtualization layer is provided by Crossbeam's XOS v9.9.0 (also referred to throughout this document as the hypervisor), which runs over a Linux-based host operating system on Crossbeam's APM blade installed in one of a Crossbeam X-Series chassis. The module was tested and found to be compliant with FIPS 140-2 requirements on an operational environment consisting of the following hardware components:

- Crossbeam Application Processor Module APM-9600 blade with two (2) Intel Xeon processors
- Crossbeam X80-S AC chassis

The module interacts directly with the hypervisor.

The module implements three software cryptographic libraries to offer cryptographic functionalities. The software libraries for the module are:

- McAfee Firewall Enterprise 32-bit Cryptographic Engine (Virtual) v8.3
- McAfee Firewall Enterprise 64-bit Cryptographic Engine (Virtual) v8.3
- Kernel Cryptographic Library for SecureOS® (KCLSOS) Version 8.2

Security functions offered by the libraries in the module's Approved mode of operation (and their associated algorithm implementation certificate numbers) are listed in Table 2.

Table 2 – Approved Security Functions

Approved Security Function	32-bit	64-bit	KCLSOS
Symmetric Key			
Advanced Encryption Standard (AES) 128/192/256-bit in CBC[7], ECB[8], OFB[9], CFB128[10] modes	2304	2306	-

[6] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[7] CBC – Cipher-Block Chaining

Approved Security Function	32-bit	64-bit	KCLSOS
AES 128/192/256-bit in CBC, ECB modes	-	-	1963
Triple Data Encryption Standard (DES) 2- and 3-key options in CBC, ECB, OFB, CFB64 modes	1452	1454	-
Triple-DES 2- and 3-key options in CBC mode	-	-	1275
Asymmetric Key			
RSA[11] ANSI X9.31 key generation: 2048/3072/4096-bit	1188	1190	-
RSA PKCS #1 signature generation: 2048/3072-bit	1188	1190	-
RSA PKCS #1 signature verification: 1024/1536/2048/3072/4096-bit	1188	1190	-
Digital Signature Algorithm (DSA) signature verification: 1024-bit	723	725	-
Secure Hash Standard			
SHA[12]-1, SHA-256, SHA-384, and SHA-512	1989	1991	1722
Message Authentication			
HMAC[13] using SHA-1, SHA-256, SHA-384, and SHA-512	1419	1421	1184
Random Number Generators (RNG)			
ANSI[14] X9.31 Appendix A.2.4 PRNG	1147	1149	1032
Key Agreement Scheme (KAS)			
Diffie-Hellman (DH): 2048-bit[15]	Non-approved, but allowed	Non-approved, but allowed	-
Key Transport			
RSA encrypt/decrypt[16] 2048/3072-bit	Non-approved, but allowed	Non-approved, but allowed	-

***NOTE**: The following algorithms listed in the table above are considered "restricted" or "legacy-use". For details regarding algorithm deprecation, please refer to NIST Special Publication 800-131A.*

- *Two-key Triple DES[17]*
- *1024-bit DSA digital signature verification*
- *1024/1536-bit RSA digital signature verification*

The module also includes the following non-compliant algorithms:

- 1024/1536/4096-bit RSA PKCS #1 signature generation
- 1024/1536/4096-bit RSA ANSI X9.31 key generation

[8] ECB – Electronic Codebook
[9] OFB – Output Feedback
[10] CFB128 – 128-bit Cipher Feedback
[11] RSA – Rivest, Shamir, and Adleman
[12] SHA – Secure Hash Algorithm
[13] HMAC – (Keyed-) Hash Message Authentication Code
[14] ANSI – American National Standards Institute
[15] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
[16] Caveat: RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
[17] Caveat: To use the two-key Triple DES algorithm to encrypt data (or wrap keys) in an Approved mode of operation, the module operator shall ensure that the same two-key Triple DES key is not used for encrypting data (or wrapping keys) with more than 2^{20} plaintext data (or plaintext keys).

- 1024-bit Diffie-Hellman
- 1024/1536/4096-bit RSA encrypt/decrypt

Additionally, the module employs a hardware RNG which acts as an entropy-gathering mechanism to provide seeding material for KCLSOS PRNG.

The module also includes two library/executable collections that provide the key derivation function (KDF) implementations for the various protocols. These engines provide KDF functionality to both 32-bit and 64-bit applications resident on the module. They are:

- McAfee Firewall Enterprise 32-bit Protocol Engine (Virtual) v8.3
- McAfee Firewall Enterprise 64-bit Protocol Engine (Virtual) v8.3

Table 3 lists the key derivation functions (and their associated CVL[18] certificate numbers) implemented by the module.

Table 3 – Approved Key Derivation Functions

Approved KDF	32-Bit Protocol Engine	64-Bit Protocol Engine
Transport Layer Security (TLS) v1.0	#127	#129
Secure Shell (SSH)	#127	-
Internet Key Exchange (IKE) v1 and v2	#127	-
Simple Network Management Protocol (SNMP) v3	-	#129

2.2.1 Physical Cryptographic Boundary

As a software module, the virtual appliance has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the hard enclosure around the host platform on which it runs. This module is intended to run on a Crossbeam APM-9600 blade populated in a Crossbeam X80-S AC Platform chassis. Figure 2 below shows the chassis.

[18] CVL – Component Validation List

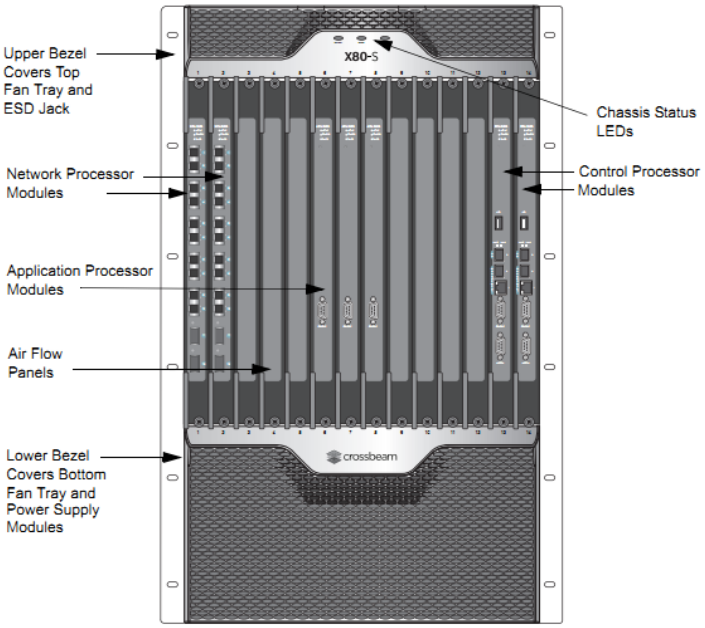

Figure 2 – Crossbeam X80-S AC Platform

The module's physical cryptographic boundary is further illustrated by the black dotted line in Figure 3 below.

The module makes use of the physical interfaces of the computing platform hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the MFE for Crossbeam and the operator, and is responsible for mapping the module's virtual interfaces to the host platform's physical interfaces. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM[19], hard disk, device case, power supply, and fans.

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the module (shown by the red dotted line in Figure 3 below) consists of the McAfee Firewall Enterprise application, three cryptographic libraries, and McAfee's SecureOS® v8.3 acting as the guest OS.

[19] RAM – Random Access Memory

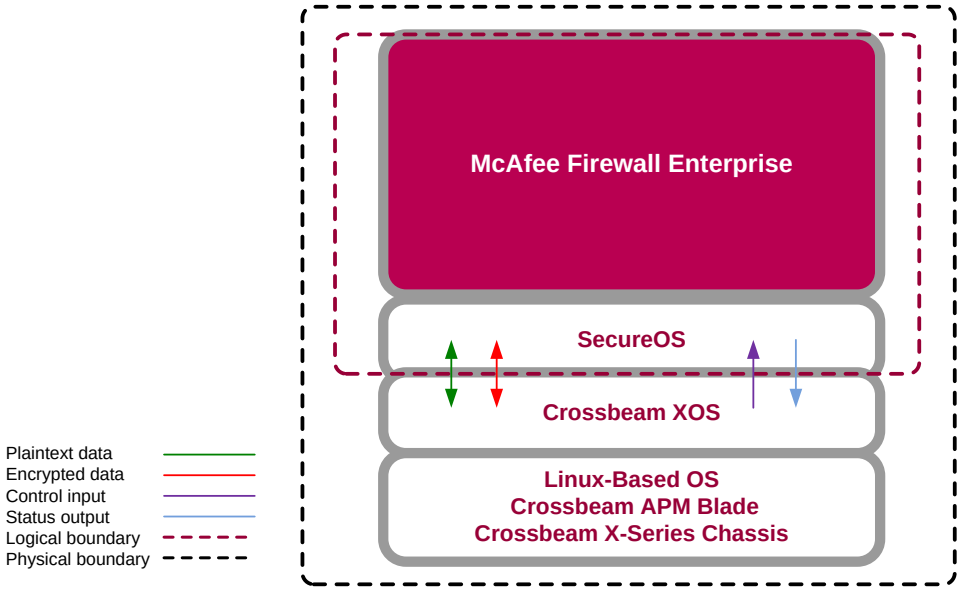

Figure 3 – MFE for Crossbeam Cryptographic Boundaries

2.3 Module Interfaces

Interfaces on the module can be categorized as the following FIPS 140-2 logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

The module's physical and electrical characteristics, manual controls, and physical indicators are provided by the host platform; the hypervisor provides virtualized ports and interfaces which map to the host platform's physical ports and interfaces. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 4 below.

Table 4 – Virtual Appliance Interface Mappings

Physical Port/Interface	Virtual Port/Interface	FIPS 140-2 Logical Interface
NPM Ethernet ports	Virtual Ethernet ports	• Data Input • Data Output
NPM LEDs	Virtual LEDs	• Status Output
CPM Ethernet ports	Virtual Ethernet ports	• Control Input • Status Output
CPM SFP ports	Virtual SFP ports	• Control Input • Status Output
CPM serial ports	Virtual serial ports	• Control Input • Status Output

Physical Port/Interface	Virtual Port/Interface	FIPS 140-2 Logical Interface
CPM USB port	Virtual USB port	• Control Input • Status Output
CPM reset switch	N/A	• Control Input
APM LEDs	Virtual LEDs	• Status Output
APM reset switch	N/A	• Control Input

Data input and output are the packets utilizing the services provided by the module. These packets enter and exit the module through the virtual Ethernet ports. Control input consists of configuration or administrative data entered into the module. Status output consists of the status provided or displayed via the operator interfaces (such as the GUI or CLI), indicators, or available log information.

2.4 Roles, Services, and Authentication

The following sections described the authorized roles supported by the module, the services provided for those roles, and the authentication mechanisms employed.

2.4.1 Authorized Roles

There are two authorized roles in the module that an operator may assume: a Crypto-Officer (CO) role and a User role.

- Crypto-Officer Role – The Crypto-Officer role performs administrative services on the module, such as initialization, configuration, and monitoring of the module.

- User Role – Users employ the services of the modules for establishing VPN[20] or TLS connections via Ethernet port.

2.4.2 Services

The services that require operators to assume an authorized role (Crypto-Officer or User) are listed in Table 5 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 5 use the following indicators to show the type of access required:

- **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

[20] VPN – Virtual Private Network

Table 5 – Authorized Operator Services

Service	Description	Role		CSP and Type of Access
		CO	User	
Authenticate to the Admin Console	Allows administrators to login to the appliance using the Firewall Enterprise Admin Console	x		Administrator Password - R
Authenticate to the Admin Console using Common Access Card (CAC)	Allows administrators to login to the appliance with CAC authentication to access the Firewall Enterprise Admin Console	x		Administrator Password - R
Authenticate to the Admin CLI	Allows administrators to login to the appliance using the Firewall Enterprise Admin CLI	x		Administrator Password - R
Authenticate to the Admin CLI using CAC	Allows administrators to login to the appliance with CAC authentication to access the Firewall Enterprise Admin CLI	x		Administrator Password - R
Authenticate to the local console	Allows administrators to login to the appliance via the local console	x		Administrator Password - R
Change password	Allows external users to use a browser to change their Firewall Enterprise, SafeWord PremierAccess, or LDAP login password	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrator Password - R/W
Manage network objects	Allows administrators to view, create, and maintain network objects, manage netgroup memberships, and manage access control rules' time periods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure identity validation method	Allows administrators to select identity validation settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure cluster communication	Provides services required to communicate with each other in Firewall Enterprise multi-appliance configurations	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	Role		CSP and Type of Access
		CO	User	
Configure and monitor Virtual Private Network (VPN) services	Generates and exchanges keys for VPN sessions	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W IKE Preshared key - W IPsec Session Key - W IPsec Authentication Key - W
Create and configure bypass mode	Creates and monitors IPsec policy table that governs alternating bypass mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage web filter	Manages configuration with the SmartFilter	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage Control Center communication	Verifies registration and oversees communication among the Control Center and managed Firewall Enterprise appliances	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure Network Integrity Agent (NIA) settings	Configures NIA authentication and certificate settings, enable agent discovery, modify connection settings, and create explicit NIA communication rules	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure content inspection settings	Configures settings for content inspection methods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage applications and Application Defense information	Manages applications, application groups, and Application Defense settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage access control rules	Manages rules enforcing policy on network flows to or through the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage SSL rules	Manages SSL rules for processing SSL connections	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	Role		CSP and Type of Access
		CO	User	
Process audit data	Allows administrators to view and export audit data, transfer audit records, and manage log files.	x		Firewall Authentication Keys - R Key Agreement Key - R DTLS Session Authentication Key - R/W DTLS Session Key - R/W
Manage attack and system responses	Configures how the firewall should respond to audit events that indicate abnormal and potentially threatening activities	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure network defenses	Customizes audit output for attacks on specific networks stopped by the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
View active hosts	Provides a method to view active hosts connected to a Firewall Enterprise appliance	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Monitor status via SNMP	Monitors non-FIPS relevant status of the module via SNMP v3	x		SNMP v3 Session Key - R
Configure networking	Configures and manages network characteristics, security zones, and Quality of Service profiles.	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage email services	Manages email options and 'sendmail' features	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Perform self-tests	Run self-tests on demand via reboot	x		None
Enable FIPS mode	Configures the module in FIPS mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Show status	Allows Crypto-Officer to check whether FIPS mode is enabled	x		None
Zeroize	Resets the module to its factory default state	x		Common Access Card Authentication keys - R/W Firewall Authentication public/private keys - R/W Peer public keys - R/W Local CA public/private keys - R/W IKE Preshared Key - R/W IPsec Session Authentication Key - R/W Administrator Password - R/W SSL CA key - R/W SSL Server Certificate key - R/W

Service	Description	Role		CSP and Type of Access
		CO	User	
Establish an authenticated TLS connection	Establish a TLS connection (requires operator authentication)		x	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W SSL CA key - R SSL Server Certificate key - R
Establish a VPN connection	Establish a VPN connection over IPsec tunnel		x	Firewall Authentication Keys - R Key Agreement Key - R IKE Session Authentication Key - W IKE Session Key - W IKE Preshared Key - R IPsec Session Key - R/W IPsec Authentication Key - R/W

2.4.3 Authentication Mechanisms

The MFE for Crossbeam supports role-based authentication. Module operators must authenticate to the module before being allowed access to services which require the assumption of an authorized role. The module employs the authentication methods described in Table 6 to authenticate Crypto-Officers and Users.

Table 6 – Authentication Mechanisms Employed by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is $1:94^8$, or 1: 6,095,689,385,410,816. This would require about 60,956,893,854 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.
	Common Access Card	One-time passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 128 characters. The password consists of a modified base-64 alphabet, which gives a total of 64 characters to choose from. With the possibility of using repeating characters, the chance of a random attempt falsely succeeding is $1:64^8$, or 1:281,474,976,710,656. This would require about 2,814,749,767 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. At that rate, and assuming no overhead, a maximum of only 937,500,000 8-character passwords can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.

Role	Type of Authentication	Authentication Strength
User	Password or Certificate	Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is $1:94^8$, or 1: 6,095,689,385,410,816. This would require about 60,956,893,854 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding. Certificates used as part of TLS, SSH, and IKE[21]/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is $1:2^{80}$, or 1: 1.20893×10^{24}. The fastest network connection supported by the module is 1000 Mbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. The passwords are sent to the module via security protocols IPsec, TLS, and SSH. These protocols provide strong encryption (AES 128-bit key at minimum, providing 128 bits of security) and require large computational and transmission capability. The probability that a random attempt will succeed or a false acceptance will occur is less than $1:2^{128} \times 84^4$.

2.5 Physical Security

McAfee Firewall Enterprise Virtual Appliance for Crossbeam 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 module was tested and found to be compliant with FIPS 140-2 requirements on an operational environment consisting of the following components:

- Crossbeam Application Processor Module APM-9600 blade with two (2) Intel Xeon processors
- Crossbeam X80-S AC chassis
- Crossbeam XOS v9.9.0 with McAfee's SecureOS v8.3 as a guest OS

The vendor also affirms that the module performs in a compliant manner running the operational environment listed above with the APM-9600 blade populated in the Crossbeam X60 chassis. However, the CMVP makes no statement as to the correct operation of the module or the security strengths of the

[21] IKE – Internet Key Exchange

generated keys when so ported if the specific operational environment is not listed on the validation certificate.

All cryptographic keys and CSPs are under the control of the guest operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 7. Note that the module generates cryptographic keys whose strengths are modified by available entropy. The available entropy is in the range of 114-128 bits.

.

Table 7 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Session Key	AES 128-bit CFB key	Internally generated using a non-compliant method	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Provides secured channel for SNMPv3 management
Common Access Card Authentication keys	RSA 2048-bit key DSA 2048-bit key	Imported electronically in plaintext	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Common Access Card Authentication for generation of one-time password
Firewall Authentication public key	RSA 2048-bit key	Internally generated	Output in encrypted form via network port or in plaintext form via local management port	Stored in plaintext on the hard disk	Erasing the system image	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
	RSA 2048-bit key	Imported electronically in plaintext via local management port	Never exits the module	Resides in volatile memory in plaintext	Erasing the system image	
Firewall Authentication private key	RSA 2048-bit key	Internally generated	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
Peer public key	RSA 2048-bit key	Imported electronically in plaintext during handshake protocol	Never exit the module	Stored in plaintext on the hard disk	Erasing the system image	Peer Authentication for TLS, SSH, and IKE sessions
Local CA[22] public key	RSA 2048-bit key	Internally generated	Public key certificate exported electronically in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Local signing of firewall certificates and establish trusted point in peer entity

[22] CA – Certificate Authority

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Local CA private key	RSA 2048-bit key	Internally generated	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Local signing of firewall certificates and establish trusted point in peer entity
Key Agreement Key	Diffie-Hellman 2048-bit key RSA 2048/3072-bit key	Internally generated	Public exponent electronically in plaintext, private component not exported	Resides in volatile memory in plaintext	Power cycle or session termination	Key exchange/agreement for DTLS, TLS, IKE/IPsec and SSH sessions
TLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for TLS sessions
TLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for TLS sessions
DTLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for DTLS sessions
DTLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for DTLS sessions
IKE Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for IKE sessions
IKE Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for IKE sessions
IKE Preshared Key	Triple-DES, AES-128, AES-256 key	- Imported in encrypted form over network port or local management port in plaintext - Manually entered	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Data encryption/decryption for IKE sessions

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IPsec Session Authentication Key	HMAC SHA-1 key	- Imported in encrypted form over network port or local management port in plaintext - Internally generated - Manually entered	Never exits the module	- Stored in plaintext on the hard disk - Resides in volatile memory	Power cycle	Data authentication for IPsec sessions
IPsec Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Data encryption/decryption for IPsec sessions
IPsec Preshared Session Key	Triple-DES, AES-128, AES-256 key	- Imported in encrypted form over network port or local management port in plaintext - Manually entered	Exported electronically in plaintext	Stored in plaintext on the hard disk	Power cycle	Data encryption/decryption for IPsec sessions
SSH Session Authentication Key	HMAC-SHA1 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for SSH sessions
SSH Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for SSH sessions
Package Distribution Public Key	DSA 1024-bit public key	Externally generated and hard coded in the image	Never exits the module	Hard coded in plaintext	Erasing the system image	Verifies the signature associated with a firewall update package
License Management Public Key	DSA 1024-bit public key	Externally generated and hard coded in the image	Never exits the module	Hard coded in plaintext	Erasing the system image	Verifies the signature associated with a firewall license
Administrator Password	PIN	Manually or electronically imported	Never exits the module	Stored on the hard disk through one-way hash obscurement	Erasing the system image	Standard Unix authentication for administrator login

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Common Access Card One-Time Password	8-character (minimum) ASCII string	Internally generated; Manually or electronically imported	Exported electronically in encrypted form over TLS	Resides in volatile memory inside the CAC Warder process	Password expiration, session termination, or power cycle	Common Access Card authentication for administrator login
MFE CE32 ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE32 ANSI X9.31 PRNG Key	AES-256 key	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE64 ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE64 ANSI X9.31 PRNG Key	AES-256 key	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
KCLSOS ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated from entropy sources	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
KCLSOS ANSI X9.31 PRNG Key	AES-256 key	Internally generated from entropy sources	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
SSL CA Key	RSA 2048-bit key DSA 2048-bit key	Internally generated	Exported electronically in ciphertext via network port or in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Signing temporary server certificates for TLS re-encryption
SSL Server Certificate Key	RSA 2048-bit key DSA 2048-bit key	Internally generated or imported electronically in plaintext via local management port	Exported electronically in ciphertext via network port or in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Peer authentication for TLS sessions (TLS re-encryption)

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

At power-up, the MFE for Crossbeam automatically performs a software integrity check using HMAC SHA-256. The module also conducts cryptographic algorithm tests at power-up in the form of Known Answer Tests (KAT) and Pairwise Consistency Tests as list in Table 8 (note that the table indicates the library with which each test is associated).

Table 8 – Power-Up Cryptographic Algorithm Self-Tests

Algorithm Self-Test	32/64-Bit	KCLSOS
AES KAT for encrypt/decrypt	✓	✓
Triple-DES KAT for encrypt/decrypt	✓	✓
RSA KAT for sign/verify	✓	-
RSA KAT for encrypt/decrypt	✓	-
DSA pairwise consistency check	✓	-
SHA-1 KAT, SHA-256 KAT, SHA-384 KAT, and SHA-512 KAT	✓	✓
HMAC KAT with SHA-1, SHA-256, SHA-384, and SHA-512	✓	✓
ANSI X9.31 Appendix A.2.4 PRNG KAT	✓	✓

If any of the tests listed above fails to perform successfully, the module enters into a critical error state during which all cryptographic operations and output of any data is inhibited. An error message is logged for the CO to review and requires action on the Crypto-Officer's part to clear the error state.

2.8.2 Conditional Self-Tests

The McAfee Firewall Enterprise Virtual Appliance for Crossbeam conducts conditional cryptographic algorithm self-tests as indicated in Table 9 (again, note that the table indicates the library with which each test is associated).

Table 9 – Conditional Self-Tests

Algorithm Self-Test	32/64-Bit	KCLSOS
Continuous RNG Test (CRNGT)	✓	✓
RSA pairwise consistency test	✓	-
DSA pairwise consistency test	✓	-

The module also performs the following conditional self-tests during module operation:

- Manual key entry test
- Bypass test using SHA-1
- Software Load Test using DSA signature verification

Failure of the Bypass test or the KCLSOS PRNG CRNGT implementation leads the module to a critical error state. Failure of any other conditional test listed above leads the module to a soft error state and logs an error message.

Upon reaching the critical error or soft error state, all cryptographic operations and data output is inhibited.

2.8.3 Critical Functions Self-Test

The McAfee Firewall Enterprise Virtual Appliance for Crossbeam performs the following critical functions self-test at power-up:

- License Verification check

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The McAfee Firewall Enterprise Virtual Appliance for Crossbeam meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in its Approved mode of operation.

Caveat: This guide assumes that the Crossbeam X-Series Platform has been installed and configured according to the proper hardware installation guide, and that a virtual environment is already setup and ready for accepting a new virtual appliance installation.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for installation, initialization, and security-relevant configuration and management of the module. Please see McAfee's Administration Guide for more information on configuring and maintaining the module.

3.1.1 Installation

The cryptographic module requires that the proper version be installed on the target hardware. The Crypto-Officer must have a McAfee-provided grant number in order to download the required image. Grant numbers are sent to McAfee customers via email after the purchase of a McAfee product.

3.1.1.1 Installation

To download and install Firewall Enterprise version 8.3.1 onto a Crossbeam X-Series platform, the Crypto-Officer must:

1. Download the Firewall Enterprise installer package.
   a. In a web browser, navigate to www.mcafee.com/us/downloads.
   b. Enter the grant number, and then navigate to the appropriate product and version.
   c. Download the Crossbeam installer (.cbi) file.
2. Download Firewall Enterprise documentation.
   a. Go to the McAfee Technical Support Service Portal at www.mysupport.mcafee.com.
   b. Under **Self Service**, click **Product Documentation**.
   c. Select the appropriate product and version.
   d. Download the *McAfee Firewall Enterprise Product Guide, McAfee Firewall Enterprise 8.3.1 on Crossbeam X-Series Platforms Installation Guide*, and *McAfee Firewall Enterprise 8.3.1 Release Notes*.
3. Install MFE for Crossbeam according to the instructions in the downloaded Installation Guide.

3.1.2 Initialization

The Crypto-Officer is responsible for initialization and security-relevant configuration and management activities for the module through the management interfaces. Initialization and configuration instructions for the module can also be found in the *McAfee Firewall Enterprise 8.3.1 on Crossbeam X-Series Platforms Installation Guide* and this FIPS 140-2 Security Policy. The initial Administration account, including username and password for authentication to the module, is created during the startup configuration using the Quick Start Wizard.

The module must first be added and registered to the Control Center in order for it to be used for management functions. Then, the Crypto-Officer must set FIPS processing enforcement to ensure that the module uses only FIPS-Approved cryptographic functions. Finally, new certificates must be created.

Once these initialization steps are completed, the module is in its Approved mode of operation.

.

3.1.2.1 Add and Register the Module to Control Center

Perform the following steps to add and register the module to Control Center (note that this must be accomplished using the procedures for clusters):

1. Select "**Policy**" in the Control Center navigation bar.
2. Double-click the "**Clusters**" node in the Policy pane. This will launch the **Add New Cluster Wizard**.
3. Enter the connection information requested for the MFE, then click "**Next**".

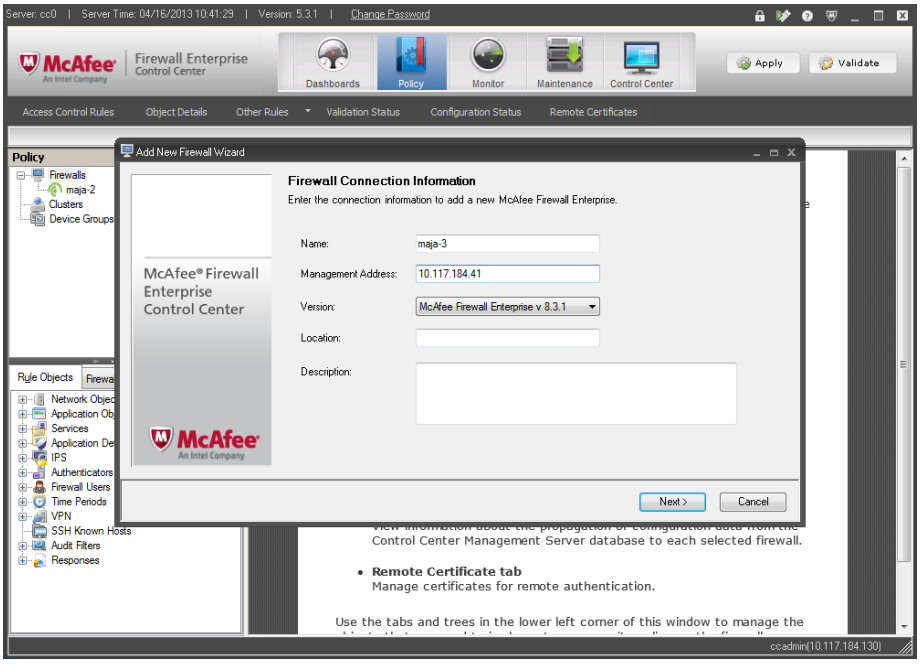

Figure 4 – Firewall Connection Information Window

4. Configure the SSH username and password, ensure that the "**Register**" option is checked, then click "**Next**".
5. A configuration summary will be displayed. Confirm the information is correct, then click "**Register**".
6. When registration is complete, click "**Next**".
7. Select the desired items and categories to be retrieved from the firewall into Control Center, then click "**Finish**".
8. A confirmation window appears. Click "**OK**" to continue.

The firewall should now appear under "**Clusters**" in the "**Policy**" pane.

3.1.2.2 Set FIPS Processing Enforcement

The CO must first check that no non-Approved service is running on the module. Services and proxies are automatically enabled when rules are created that reference those services/proxies. To view the services that are currently used in enabled rules, select "**Policy**" in the Control Center navigation bar. Then right-click on the module node in the Policy tree and select the "**View Rules**" tab. This will display the **Access Control Rules** page.

If the Active Rules popup lists any non-Approved protocols (such as telnet), then those protocols must be disabled before the module is considered to be in its Approved mode of operation. To change a given rule, select the rule, then click "**Edit**". After making the appropriate changes, click "**OK**" to save the rule.

The process to enable FIPS processing as follows:

1. Right-click the module node in the **Policy** pane in the Control Center GUI and select "**Edit Cluster Settings**". This will open a "**General**" window.
2. Expand "**Settings**" in the left pane and select "**Other**". This will display the "**Other**" tab in the right pane.
3. Ensure that the "**Require FIPS 140-2 processing**" option is checked, then click **OK** (see figure 3).

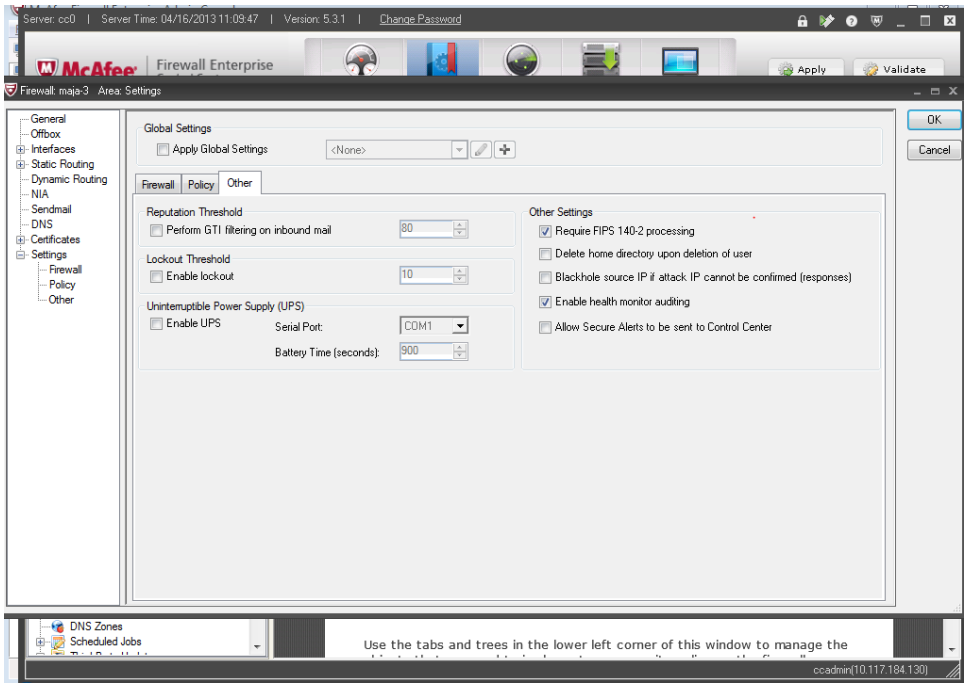

Figure 5 – Control Center GUI (with FIPS enforcement checkbox selected)

4. A confirmation window may appear. Click **OK** to continue. This will display the Control Center's default screen.
5. Click **Apply**. This will display a screen where you must select the firewalls on which to apply the current configuration.
6. Select the module hostname from the firewall list, then click **OK**. After the change is applied to the module, the Control Center's default screen will be displayed.
7. Reboot the module to activate the change.
    a. Select "**Configuration Status**" on the Control Center toolbar, then select "**Current**" from the Display Configurations dropdown menu. Control Center will display all current hosts.
    b. Select "**Maintenance**" from the toolbar and double-click "**Device Control**" in the **Maintenance** pane. This will display a device control window.

c. Select the module's hostname, ensure that the "**System shutdown/reboot**" dropdown menu option is selected, then click **Proceed**. This will display a device confirmation window.
d. Confirm that the module was selected, then click **OK**. The module will reboot.

To confirm that FIPS enforcement has been activated for the module, follow the guidance in Section 3.1.3.1 below.

3.1.2.3 Configure SSL Rules

The Crypto-Officer shall ensure that the module's client-to-firewall and firewall-to-server decryption policies are set properly and employ the correct version of TLS for communications. From the Control Center toolbar, the CO must select "**Other Rules**" and ensure that the actions associated with each SSL rule defined for the module are set to either "**Decrypt only**" or "**Decrypt/Re-encrypt**". Additionally, the CO must ensure that the rules allow for SSL connections using TLSv1 only. For details regarding editing SSL rules, please refer to the "Add or edit an SSL rule" section of the *McAfee Firewall Enterprise Control Center v5.3.1 Product Guide*.

3.1.2.4 Recreate Module Certificates

The Crypto-Officer shall delete and recreate all required cryptographic keys and CSPs necessary for the module's secure operation. The keys and CSPs existing on the module were generated outside of Approved mode, and they must now be re-created for use in FIPS mode. The CO must replace the certificates/CSPs listed in Table 10.

Table 10 – Certificates and CSPs Required for Secure Operation

Services	Certificates and CSPs
Control Center (TLS)	Firewall Certificate/private key
HTTPS[23] Decryption (TLS)	Firewall Certificate/private key
TrustedSource (TLS)	Firewall Certificate/private key
Firewall Cluster Management (TLS)	Firewall Certificate/private key Local CA/private key
Passport Authentication (TLS)	Firewall Certificate/private key
IPsec/IKE certificate authentication	Firewall Certificate/private key
Audit log signing	Firewall Certificate/private key
SSH server	Firewall Certificate/private key
Administrator Passwords	Firewall Certificate/private key

For details regarding creating new certificates, please refer to the "Certificates" chapter of the *McAfee Firewall Enterprise Control Center v5.3.1 Product Guide*

3.1.3 Management

Once properly configured according to the Crypto-Officer guidance in this Security Policy, the module supports the use of Approved services only. The Crypto-Officer is able to monitor and configure the module via the MFE Control Center, CLI over SSH, serial port, or direct-connected keyboard/monitor. Detailed instructions to monitor and troubleshoot the systems are provided in the *McAfee Firewall*

[23] HTTPS – Hypertext Transfer Protocol Secure

Enterprise 8.3.1 Product Guide. The Crypto-Officer should monitor the module's status regularly for Approved mode of operation and active bypass mode.

If any irregular activity is noticed or the module is consistently reporting errors, then McAfee customer support should be contacted.

3.1.3.1 Monitoring Status

The Crypto-Officer may determine the module's current mode of operation by double-clicking the module hostname in the Control Center GUI **Policy** Pane and selecting "**Launch Secure Shell**". After connecting, the CO must enter the following two commands on the command line:

```
% srole
% cf fips query
```

When correctly configured, the module will display the following message:

```
fips set enabled=yes
```

The Crypto-Officer may determine the module's bypass mode status via the Control Center GUI. The CO must navigate to the **VPN / VPN Bypass** branch under the **Rule Object** tab of the **Policy** pane. This will display a listing of any firewalls with associated bypass rules. Additionally, the Crypto-Officer may enter "***cf ipsec q type=bypass***" via the shell to get a listing of the existing bypass rules, while "***cf package list***" will provide the module version number.

The Crypto-Officer should monitor the module's status regularly for Approved mode of operation and active bypass mode. If any irregular activity is noticed or the module is consistently reporting errors, then McAfee customer support should be contacted.

3.1.3.2 Zeroization

In order to zeroize the module of all keys and CSPs, it is necessary to first rebuild the module's image, essentially wiping out all data from the module. Once a factory reset has been performed, default keys and CSPs must be set up as part of the renewal process. These keys must be recreated as per the instructions found in Section 3.1.2.4. Failure to recreate these keys will result in a non-compliant module.

For more information about resetting the module to a factory default state, please consult the appropriate downloaded documentation for the module.

3.2 User Guidance

When using key establishment protocols (RSA and DH) in the Approved mode, the User is responsible for selecting a key size that provides the appropriate level of key strength for the key being transported.

3.3 Non-Approved Mode of Operation

When configured and initialized per the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

.

4 Acronyms

This section describes the acronyms used throughout the document.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APM	Application Processor Module
BIOS	Basic Input/Output System
CAC	Common Access Card
CBC	Cipher-Block Chaining
CD	Compact Disc
CD-ROM	Compact Disc – Read-Only Memory
CFB	Cipher Feedback
CLI	Command Line Interface
CLSOS	Cryptographic Library for SecureOS
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPM	Control Processing Module
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CVL	Component Validation List
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HA	High Availability

.

Acronym	Definition
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
KAT	Known Answer Test
KCLSOS	Kernel Cryptographic Library for SecureOS
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MAC	Message Authentication Code
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMS	Network Management System
OFB	Output Feedback
OS	Operating System
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
UTM	Unified Threat Management
VAP	Virtual Application Processor
VPN	Virtual Private Network
XOS	X-Series Operating System

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