

McAfee, Inc.

McAfee Firewall Enterprise Virtual Appliance for VMware

Software Version: 8.3.2 with patch number 8.3.2E14

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: I
Document Version: 0.4



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

1	INTRODUCTION	4
1.1	PURPOSE	4
1.2	REFERENCES	4
1.3	DOCUMENT ORGANIZATION	4
2	MFE VIRTUAL APPLIANCE	5
2.1	OVERVIEW	5
2.2	MODULE SPECIFICATION	7
2.2.1	<i>Physical Cryptographic Boundary</i>	10
2.2.2	<i>Logical Cryptographic Boundary</i>	11
2.3	MODULE INTERFACES	11
2.4	ROLES, SERVICES, AND AUTHENTICATION	12
2.4.1	<i>Authorized Roles</i>	12
2.4.2	<i>Services</i>	12
2.4.3	<i>Authentication Mechanisms</i>	16
2.5	PHYSICAL SECURITY	18
2.6	OPERATIONAL ENVIRONMENT	18
2.7	CRYPTOGRAPHIC KEY MANAGEMENT	18
2.8	SELF-TESTS	23
2.8.1	<i>Power-Up Self-Tests</i>	23
2.8.2	<i>Conditional Self-Tests</i>	23
2.9	MITIGATION OF OTHER ATTACKS	24
3	SECURE OPERATION	25
3.1	CRYPTO-OFFICER GUIDANCE	25
3.1.1	<i>Installation</i>	25
3.1.2	<i>Initialization</i>	26
3.1.3	<i>Management</i>	28
3.1.4	<i>Monitoring Status</i>	29
3.1.5	<i>Zeroization</i>	29
3.2	USER GUIDANCE	29
3.3	NON-APPROVED MODE OF OPERATION	29
4	ACRONYMS	30

Table of Figures

FIGURE 1	– TYPICAL DEPLOYMENT SCENARIO	5
FIGURE 2	– BLOCK DIAGRAM OF A TYPICAL GPC	10
FIGURE 3	– MFE VIRTUAL APPLIANCE CRYPTOGRAPHIC BOUNDARIES	11
FIGURE 4	– RULES WINDOW	26
FIGURE 5	– ACTIVE RULES WINDOW	27
FIGURE 6	– CONFIGURING FOR FIPS	28

List of Tables

TABLE 1	– SECURITY LEVEL PER FIPS 140-2 SECTION	7
TABLE 2	– APPROVED SECURITY FUNCTIONS	8
TABLE 3	– APPROVED KEY DERIVATION FUNCTIONS	9
TABLE 4	– VIRTUAL APPLIANCE INTERFACE MAPPINGS	12
TABLE 5	– AUTHORIZED OPERATOR SERVICES	13
TABLE 6	– AUTHENTICATION MECHANISMS EMPLOYED BY THE MODULE	17
TABLE 7	– CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS	19

TABLE 8 – POWER-UP CRYPTOGRAPHIC ALGORITHM SELF-TESTS	23
TABLE 9 – CONDITIONAL CRYPTOGRAPHIC ALGORITHM SELF-TESTS	23
TABLE 10 – ACRONYMS	30



Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the McAfee Firewall Enterprise Virtual Appliance for VMware from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise Virtual Appliance for VMware (Software Version: 8.3.2 with patch number 8.3.2E14) 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 VMware is referred to in this document as the MFE Virtual Appliance, 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 Virtual Appliance

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.

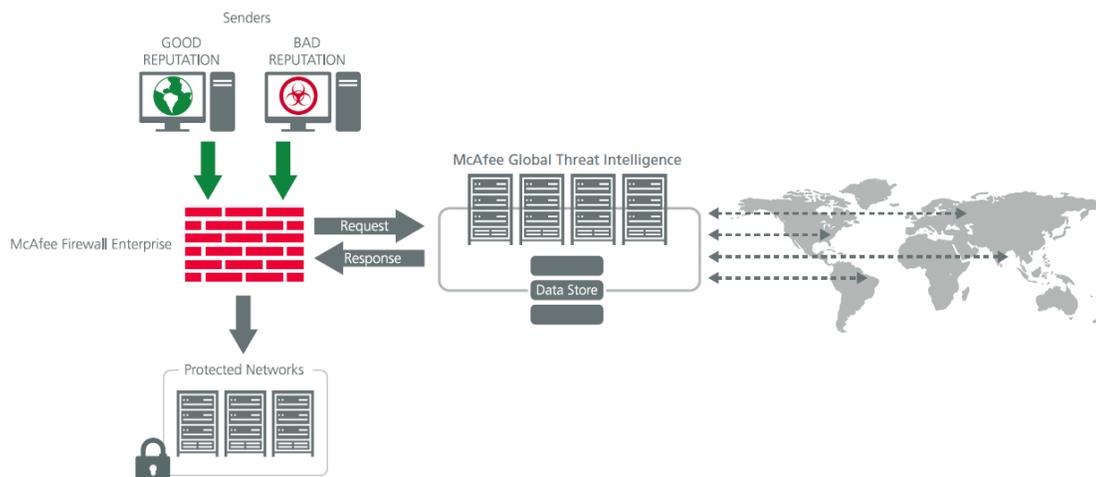


Figure 1 – Typical Deployment Scenario

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, LDAP¹, RADIUS², Windows Domain Authentication, and more
- High Availability (HA)
- Geo-location filtering
- Encrypted application filtering using TLS³ and IPsec⁴ 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 DTLS⁵ protocol

The McAfee Firewall Enterprise Virtual Appliance for VMware is designed to leverage VMware's ESXi Server virtualization technology and run the firewall as a virtual appliance installed on the server. The MFE Virtual Appliance can be managed locally or remotely using one of the following management tools:

- Administration Console – The Administration Console (or Admin Console) is the graphical software that runs on a Windows computer within a connected network. Admin Console is McAfee's proprietary GUI management software tool that needs to be installed on a Windows-based workstation. This is the primary management tool. All Admin Console sessions are protected over secure TLS channel.
- Command Line Interface (CLI) – A UNIX-based CLI is also available for configuring the firewall and performing troubleshooting functions. It can be used as an alternative to the Admin Console to perform most administration 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.
- MFE SNMP Agent – The MFE Virtual Appliance can use 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. However, the module's SNMP Agent does not support "set" requests, preventing the modification of any critical security parameters (CSPs) through this interface. Additionally, because the module's CSPs are not defined in the Firewall's MIB⁶, information about those CSPs is not made available to be transmitted or viewed over this interface. Thus, this interface provides management for non-FIPS-relevant information only, and offers no ability to alter or view CSPs.

- 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 manage their firewall solutions from the network edge to the core. Management communications between the MFE and Control Center are secured over a TLS session.

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

⁶ MIB – Management Information Base

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

The McAfee Firewall Enterprise Virtual Appliance for VMware 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
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 ⁷	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 VMware 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 guest operating system (OS) in a virtualized environment on a general-purpose computer (GPC) hardware platform.

The guest operating system is McAfee's SecureOS v8.3, while the virtualization layer is provided by VMware ESXi 5.0 (also referred to throughout this document as the hypervisor). The module interacts directly with the hypervisor, which runs directly on the GPC hardware without the need of a host OS. The module was tested and found compliant on a McAfee Firewall Enterprise S7032 appliance with Intel Xeon processor.

The module implements three software cryptographic libraries to offer secure networking protocols and cryptographic functionalities. The software libraries for the module are:

- McAfee Firewall Enterprise 32-bit Cryptographic Engine (Virtual) v8.3.2
- McAfee Firewall Enterprise 64-bit Cryptographic Engine (Virtual) v8.3.2
- Kernel Cryptographic Library for SecureOS® (KCLSOS) v8.2

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.

⁷ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Table 2 – Approved Security Functions

Approved Security Function	Certificate #		
	32-Bit	64-Bit	KCLSOS
Symmetric Key			
Advanced Encryption Standard (AES) 128/192/256-bit in CBC ⁸ , ECB ⁹ , OFB ¹⁰ , CFB128 ¹¹ , CTR ¹² modes	#2711	#2713	-
AES 128/192/256-bit in CBC, ECB modes	-	-	#1833
Triple Data Encryption Standard (DES) 2- and 3-key options in CBC, ECB, OFB, CFB64 modes	#1628	#1630	-
Triple-DES 2- and 3-key options in CBC mode	-	-	#1185
Asymmetric Key			
RSA ANSI X9.31 key generation: 2048/3072-bit	#1408	#1410	-
RSA ¹³ PKCS ¹⁴ #1 signature generation: 2048/3072-bit	#1408	#1410	-
RSA PKCS #1 signature verification: 1024/1536/2048/3072/4096-bit	#1408	#1410	-
DSA ¹⁵ PQG generation: 2048-bit	#829	#831	-
DSA PQG verification: 1024/2048/3072-bit	#829	#831	-
DSA key generation: 2048/3072-bit	#829	#831	-
DSA signature generation: 2048/3072-bit	#829	#831	-
DSA signature verification: 1024/2048/3072-bit	#829	#831	-
ECDSA ¹⁶ key generation (2048-bit); signature generation/verification (2048/256-bit)	#473	#475	-
Secure Hash Standard			
SHA ¹⁷ -1, SHA-256, SHA-384, and SHA-512	#2276	#2278	#1612
Message Authentication			
HMAC ¹⁸ using SHA-1, SHA-256, SHA-384, and SHA-512	#1690	#1692	#1086
Random Number Generators (RNG)			
ANSI ¹⁹ X9.31 Appendix A.2.4 PRNG	-	-	#964
SP 800-90 Counter-based DRBG ²⁰	#448	#450	-
Key Agreement Scheme (KAS)			

⁸ CBC – Cipher-Block Chaining⁹ ECB – Electronic Codebook¹⁰ OFB – Output Feedback¹¹ CFB128 – 128-bit Cipher Feedback¹² CTR – Counter¹³ RSA – Rivest, Shamir, and Adleman¹⁴ PKCS – Public Key Cryptography Standard¹⁵ DSA – Digital Signature Algorithm¹⁶ ECDSA – Elliptic Curve DSA¹⁷ SHA – Secure Hash Algorithm¹⁸ HMAC – (Keyed-) Hash Message Authentication Code¹⁹ ANSI – American National Standards Institute²⁰ DRBG – Deterministic Random Bit Generator

Approved Security Function	Certificate #		
	32-Bit	64-Bit	KCLSOS
Diffie-Hellman (DH): 2048 bits ²¹	Non-approved, but allowed	Non-approved, but allowed	-
Key Transport			
RSA encrypt/decrypt ²² 2048/3072-bit	Non-approved, but allowed	Non-approved, but allowed	-

NOTE: As of December 31, 2010, 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 DES²³
- 1024-bit DSA PQG verification
- 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 ANSI X9.31 key generation
- 1024/1536/4096-bit RSA PKCS #1 signature generation
- 2048/3072-bit RSA PKCS #1 signature generation with SHA-1
- 1024-bit DSA PQG generation, key generation, and signature generation
- 2048-bit DSA signature generation with SHA-1
- 1024-bit Diffie-Hellman
- 1024/1536/4096-bit RSA encrypt/decrypt

The module employs a hardware-based RNG which acts as an entropy-gathering mechanism to provide seeding material for the 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 v8.3.2
- McAfee Firewall Enterprise 64-bit Protocol Engine v8.3.2

Table 3 lists the key derivation functions (and their associated CVL²⁴ certificate numbers) implemented by the module.

Table 3 – Approved Key Derivation Functions

Approved KDF	Certificate #	
	32-Bit Protocol Engine	64-Bit Protocol Engine
Transport Layer Security (TLS) v1.0	#168	#171
Secure Shell (SSH)	#168	-

²¹ Caveat: : Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

²² Caveat: RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

²³ 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 2²⁰ plaintext data (or plaintext keys).

²⁴ CVL – Component Validation List

Approved KDF	Certificate #	
	32-Bit Protocol Engine	64-Bit Protocol Engine
Internet Key Exchange (IKE) v1 and v2	#168	-
Simple Network Management Protocol (SNMP) v3	-	#171

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 GPC on which it runs. Figure 2 shows the block diagram of a typical GPC (the dashed line surrounding the hardware components represents the module’s physical cryptographic boundary, which is the outer case of the hardware platform), and identifies the hardware with which the GPC’s processor interfaces.

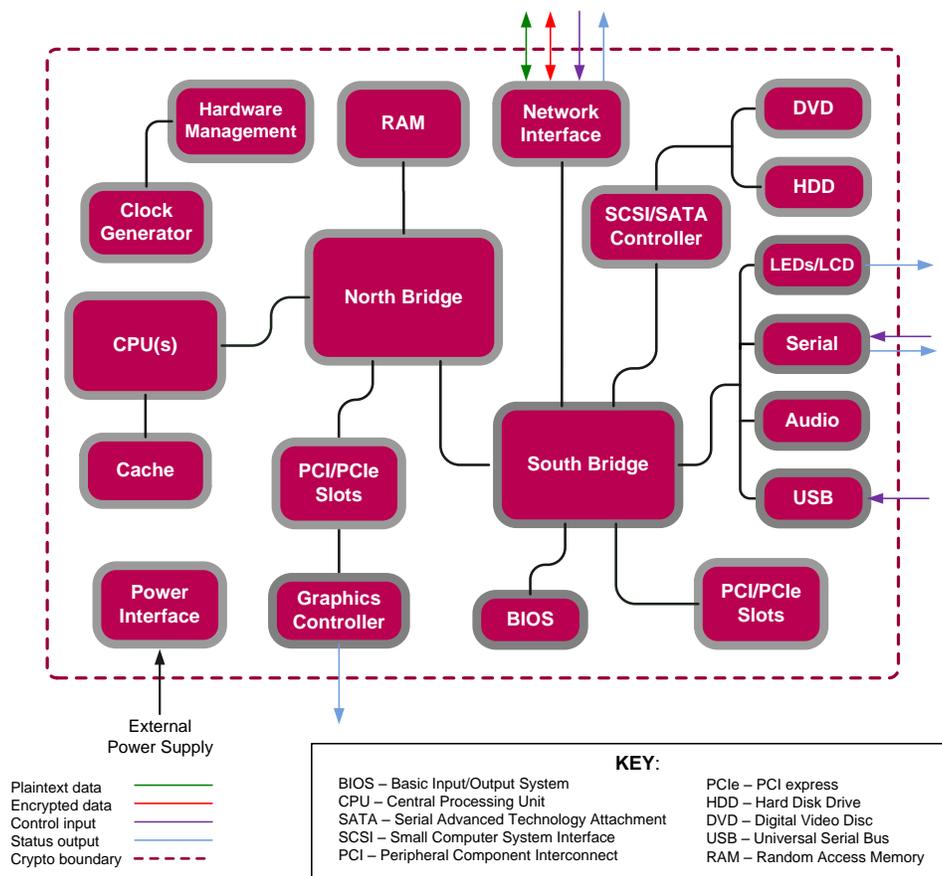


Figure 2 – Block Diagram of a Typical GPC

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 GPC hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the MFE Virtual Appliance and the operator, and is responsible for mapping the module’s virtual interfaces to the GPC’s

physical interfaces. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM²⁵, hard disk, device case, power supply, and fans. Figure 2 shows the block diagram of a typical GPC (the dashed line surrounding the hardware components represents the module's physical cryptographic boundary, which is the outer case of the hardware platform), and identifies the hardware with which the GPC's processor interfaces.

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.

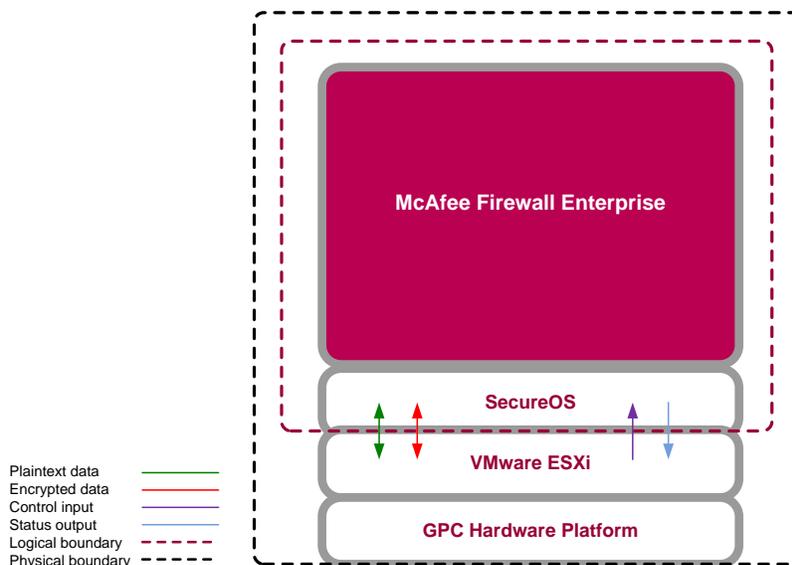


Figure 3 – MFE Virtual Appliance Cryptographic Boundaries

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 GPC; the hypervisor provides virtualized ports and interfaces which map to the GPCs' 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.

²⁵ RAM – Random Access Memory

Table 4 – Virtual Appliance Interface Mappings

Physical Port/Interface	Module Port/Interface	FIPS 140-2 Logical Interface
Host GPC Ethernet (10/100/1000) Ports	Virtual Ethernet Ports	<ul style="list-style-type: none"> • Data Input • Data Output • Control Input • Status Output
Host GPC Keyboard port	Virtual Keyboard port	<ul style="list-style-type: none"> • Control Input
Host GPC Mouse port	Virtual Mouse port	<ul style="list-style-type: none"> • Control Input
Host GPC Serial Port	Virtual Serial Port	<ul style="list-style-type: none"> • Data Input • Control Input
Host GPC Video Connector	Virtual Video Interface	<ul style="list-style-type: none"> • Status Output
Host GPC Power Interface	N/A	<ul style="list-style-type: none"> • Power

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) 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 VPN²⁶ 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

²⁶ 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 Administrative 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 Passwords - 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 Virtual Appliance 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	<p>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 1:94⁸, or 1: 6,095,689,385,410,816.</p> <p>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.</p>
	Common Access Card	<p>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 1:64⁸, or 1:281,474,976,710,656.</p> <p>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.</p>

Role	Type of Authentication	Authentication Strength
User	Password or Certificate	<p>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 1:94⁸, or 1: 6,095,689,385,410,816.</p> <p>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 × 10⁶ × 60 seconds, or 6 × 10¹⁰) 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.</p> <p>Certificates used as part of TLS, SSH, and IKE²⁷/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is 1:2⁸⁰, or 1: 1.20893 × 10²⁴.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence, at most 60,000,000,000 bits of data (1000 × 10⁶ × 60 seconds, or 6 × 10¹⁰) 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 1:2¹²⁸ × 94⁸.</p>

2.5 Physical Security

McAfee Firewall Enterprise Virtual Appliance for VMware 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 a McAfee Firewall Enterprise S7032 appliance with an Intel Xeon processor running VMware ESXi v5.0 with McAfee's SecureOS v8.3 as the guest operating system. All cryptographic keys and CSPs are under the control of the guest OS, 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.

²⁷ IKE – Internet Key Exchange

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 exits the module	Stored in plaintext on the hard disk	Erasing the system image	Peer Authentication for TLS, SSH, and IKE sessions
Local CA ²⁸ 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

²⁸ 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	<ul style="list-style-type: none"> - Imported in encrypted form over network port or local management port in plaintext - Internally generated - Manually entered 	Never exits the module	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 Virtual Appliance 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 KATs for encrypt and decrypt	✓	✓
Triple DES KATs for encrypt and decrypt	✓	✓
RSA KAT for sign and verify	✓	-
RSA KAT for encrypt and decrypt	✓	-
DSA pairwise consistency check	✓	-
ECDSA 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	✓	✓
DRBG KAT	✓	-
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 VMware 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 Cryptographic Algorithm Self-Tests

Algorithm Self-Test	32/64-Bit	KCLSOS
Continuous RNG Test (CRNGT) for PRNG	-	✓
Continuous RNG Test (CRNGT) for DRBG	✓	-
RSA pairwise consistency test for key pair generation	✓	-
DSA pairwise consistency test for key pair generation	✓	-
ECDSA pairwise consistency test for key pair generation	✓	-

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.

2.9 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 VMware 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 host platform has been installed and configured according to the proper hardware installation guide, and 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 initialization and security-relevant configuration and management of the module. Please see the *McAfee Firewall Enterprise, Virtual Appliance Installation Guide* for more information on configuring and maintaining the module.

The Crypto-Officer is also responsible for the proper initial setup of the Admin Console Management Tool software. Setup of the Admin Console software is done by installing the software on an appropriate Windows® workstation (refer to the *McAfee Firewall Enterprise version 8.3.2 Product Guide* for details regarding installation of management tools) on the same network as the module. Once the Admin Console is installed, a link to the documents page is added to the “Start” menu of the computer. To view the Firewall Enterprise documents on the McAfee web site, select

Start > Programs > McAfee > Firewall Enterprise > Online Manuals

Additional product manuals, configuration-specific application notes, and the KnowledgeBase are available at <http://mysupport.mcafee.com>.

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.

To download the Firewall Enterprise installer package, the Crypto-Officer must:

1. In a web browser, navigate to www.mcafee.com/us/downloads.
2. Enter the grant number, and then navigate to the appropriate product and version.
3. Click **View Available Downloads**, and then click the link for the latest version.
4. Click **I Agree** to accept the license agreement.
5. Download the virtual image .zip file.

To import the firmware image onto the host, the Crypto-Officer must:

1. Extract the downloaded .zip file.
2. Connect to your ESXi server using the VMware vSphere Client.
3. From the menu bar, select **File | Deploy OVF Template**. The Deploy OVF Template window appears.
4. Select the firewall file.
 - Select **“Deploy from file”**.
 - Click **Browse** to select the .ovf file you extracted.
 - Click **Next**. The **OVF Template Details** page appears.
5. Click **Next**. The **Name and Location** page appears.
6. Type a name for the firewall, and then click **Next**.
 - If the **Network Mapping** page appears, proceed to Step 7.
 - If the **Ready to Complete** page appears, proceed to Step 8.

7. On the **Network Mapping** page, verify that “**unconfigured**” is selected in the **Destination Networks** drop-down list, and then click **Next**. The **Ready to Complete** page appears.
8. Review the summary.
 - If you need to make any changes, click **Back**.
 - If the summary is correct, click **Finish**.

When you click **Finish**, the firewall is uploaded to your ESXi server.

Then, to apply the **8.3.2E14** patch, the Crypto-Officer must:

1. Log into the Admin Console.
2. Click **Maintenance**.
3. Click **Software Management**.
4. Click the **Manage Packages** tab.
5. Select the appropriate patch from the available packages table, and then click **Install**.
6. Select “Install now”, and then click **OK**.

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. The initial Administration account, including username and password for login authentication to the module, is created during the startup configuration using the Quick Start Wizard (see the *McAfee Firewall Enterprise (Multi-Firewall Edition) Quick Start Guide*). The instructions below provide the guidance necessary to initialize and configure the module using the Admin Console (additional initialization and configuration instructions for the module can be found in the *McAfee Firewall Enterprise Virtual Appliance Installation Guide*).

The Crypto-Officer must set FIPS mode enforcement to ensure that the module is running in its Approved mode of operation. Before enforcing FIPS on the module, the CO must 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 / Access Control Rules**”. The Access Control Rules window appears as shown in Figure 4 below. From here, select the “**Active Rules**” button in the upper right corner of the window (see Figure 5). If the window lists any non-Approved protocols, then those protocols must be disabled before the module is considered to be in its Approved mode of operation.

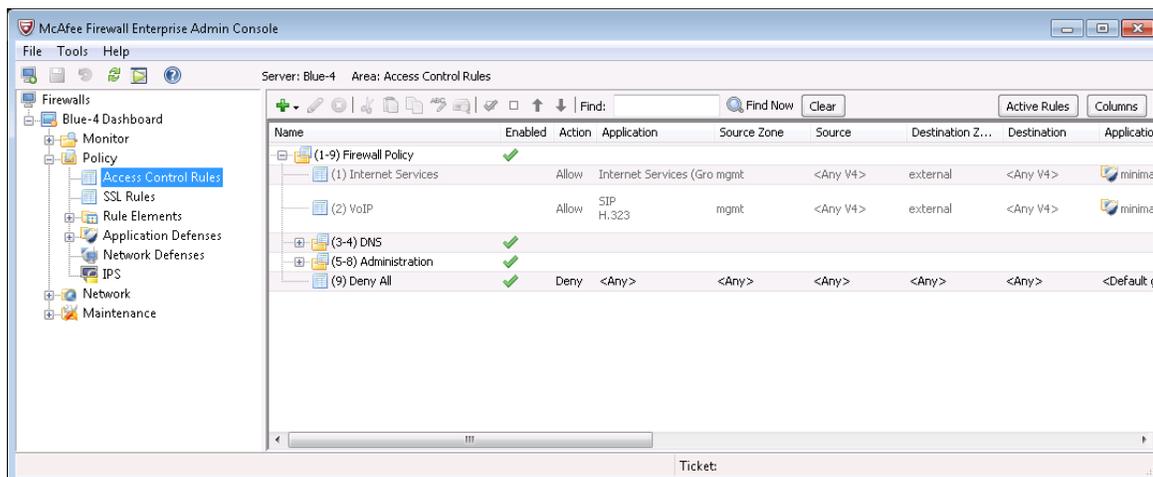


Figure 4 – Rules Window

Rules: Active Rules

Snapshot of active rules: Oct 23 2012 10:31:31 AM EDT

Position /	Name	Enabled	Action	Application	Source Zone	Source	Destination Zone
3	dnsp mgmt re...	✓	Allow	DNS	mgmt	mgmt primary DN...	external
4	dnsp all to mg...	✓	Allow	DNS	<Any>	<Any V4>	mgmt
6	Login Console	✓	Allow	Login Console	Firewall	<Any V4>	Firewall
7	Admin Console	✓	Allow	Admin Console	mgmt	<Any V4>	mgmt
9	Deny All	✓	Deny	<Any>	<Any>	<Any>	<Any>

View Export (csv) Close Help

Figure 5 – Active Rules Window

The process to enable FIPS mode is provided below:

1. Under “**Policy/Application Defenses/ Defenses/HTTPS**”, disable all non-Approved versions of SSL, leaving only TLS 1.0 operational.
2. Under “**Maintenance / Certificate Management**”, ensure that the certificates only use FIPS-Approved cryptographic algorithms.
3. Select “**Maintenance / FIPS**”. The FIPS check box appears in the right pane (shown in Figure 6).
4. Select “**Enable FIPS 140-2 processing**”.
5. Save the configuration change.
6. Select “**Maintenance / System Shutdown**” to reboot the firewall to the Operational kernel to activate the change.

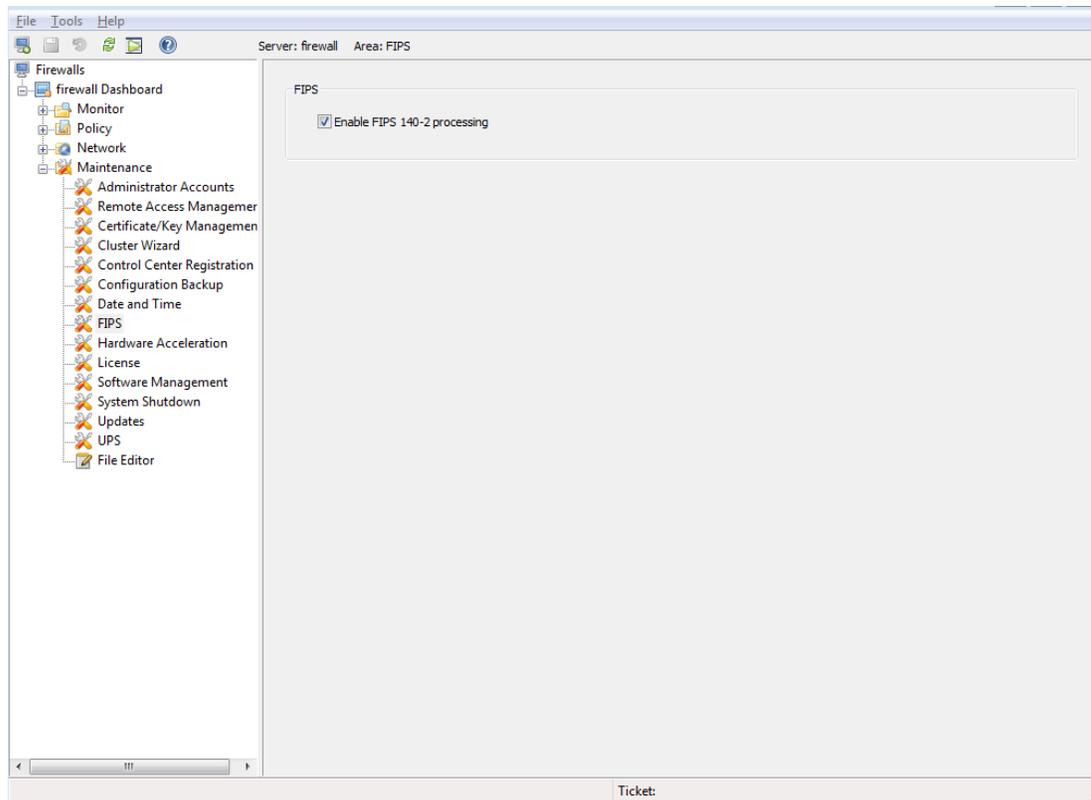


Figure 6 – Configuring For FIPS

Whether the module has been upgraded to a validated firmware version from an earlier firmware, or shipped with a validated firmware version already present, it is required to 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 the module's Approved mode of operation, and they must now be re-created for use in Approved mode. To ensure the module's secure operation, the CO shall replace the following keys and CSPs:

- Firewall Authentication private key
- Local CA private key

The module is now operating in the Approved mode of operation.

3.1.3 Management

When configured according to the Crypto-Officer guidance in this Security Policy, the module only runs in an Approved mode of operation. While in Approved mode, only Approved and Allowed algorithms may be used; the use of non-Approved algorithms is prohibited. The Crypto-Officer is able to monitor and configure the module via the web interface (GUI over TLS), SSH, serial port, or direct-connected keyboard/monitor. Detailed instructions to monitor and troubleshoot the systems are provided in the *McAfee Firewall Enterprise 8.3.2 Product Guide*. The CO must monitor that only Approved algorithms as listed in Table 2 are being used for TLS, DTLS, and SSH sessions.

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

3.1.4 Monitoring Status

The Crypto-Officer must monitor the module's status regularly for Approved mode of operation and active bypass mode.

The "show status" service to determine the current mode of operation involves examining the Admin Console's FIPS mode checkbox, shown in Figure 6. This can also be done via the following CLI command:

```
cf fips query
```

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

```
fips set enabled=yes
```

The "show status" service as it pertains to bypass is shown in the GUI under **VPN Definitions** and the module column. For the CLI, the Crypto-Officer may enter "**cf ipsec policydump**" to display the active VPNs, while "**cf ipsec q type=bypass**" will display get a listing of the existing bypass rules.

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

3.1.5 Zeroization

It is the Crypto Officer's responsibility to zeroize the module's keys when necessary. 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. 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 according to 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 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
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
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard

Acronym	Definition
GUI	Graphical User Interface
HA	High Availability
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®
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MAC	Message Authentication Code
MIB	Management Information Base
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMI	Nonmaskable Interrupt
NMS	Network Management System
OFB	Output Feedback
OS	Operating System
PCI	Peripheral Component Interconnect
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
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Acronym	Definition
USB	Universal Serial Bus
UTM	Unified Threat Management
VGA	Video Graphics Array
VPN	Virtual Private Network

Prepared by:
Corsec Security, Inc.

The logo for Corsec, featuring the word "Corsec" in a bold, dark red serif font, with a registered trademark symbol (®) to the right. The text is enclosed within a white, three-dimensional oval shape that has a subtle shadow and a slight gradient, giving it a floating appearance.

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

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