McAfee, Inc.

McAfee Firewall Enterprise Virtual Appliance for VMware ESXi v4.1

Software Version: 8.2.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: **1**
Document Version: **0.8**

Prepared for:

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

Phone: +1 (888) 847-8766
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 VMware ESXi v4.1 from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise Virtual Appliance for VMware ESXi v4.1 (Software Version: 8.2.1) 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 VMware ESXi v4.1 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 appliances have been 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, McAfee's Firewall Enterprise appliances are the strongest self-defending perimeter firewalls in the world. Built with a comprehensive combination of high-speed application proxies, McAfee's TrustedSource™ reputation-based global intelligence, and signature-based security services, Firewall Enterprise defends networks and Internet-facing applications from all types of malicious threats, both known and unknown.

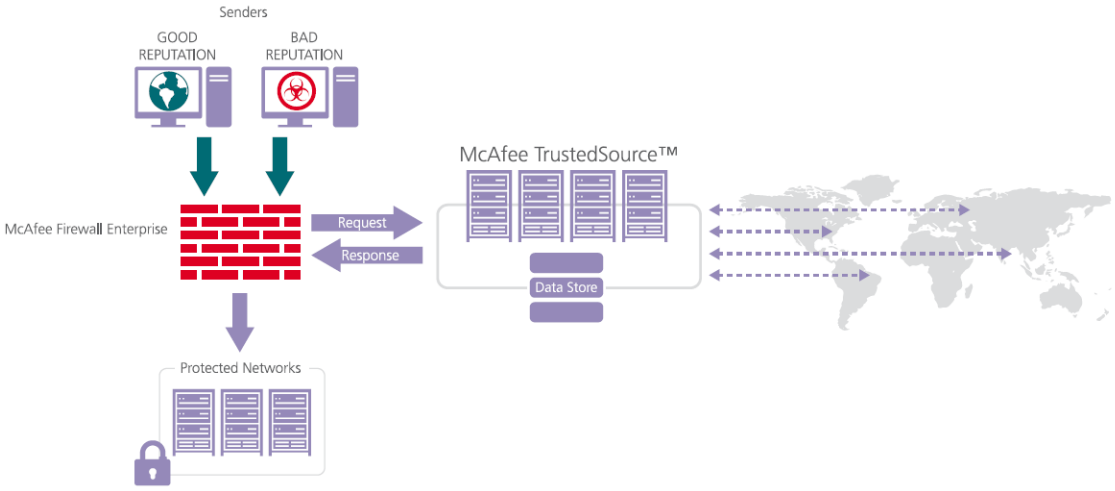

Figure 1 – Typical Deployment Scenario

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

A Firewall Enterprise appliance is managed using a proprietary graphical user interface (GUI), referred as Admin Console, and a command line management interface. Hundreds of Firewall Enterprise appliances can be managed centrally using McAfee's Control Center tool. 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

The McAfee Firewall Enterprise Virtual Appliance for VMware ESXi v4.1 is designed to leverage VMware's ESXi Server virtualization technology and run the firewall as a virtual appliance installed on the server. The McAfee Firewall Enterprise Virtual Appliance for VMware ESXi v4.1 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	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[5]	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 ESXi v4.1 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 typical general-purpose computer (GPC) hardware platform. The guest operating system is McAfee's SecureOS v8.2, while the virtualization layer is provided by VMware ESXi v4.1 (also referred to throughout this document as the

[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] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

hypervisor). The module interacts directly with the hypervisor, which runs directly on the hardware without the need of a host OS.

The module was tested and found to be compliant with FIPS 140-2 requirements in an operational environment consisting of the following components:

- Intel Xeon processor
- VMware ESXi v4.1 with McAfee's SecureOS v8.2 as the guest OS
- McAfee Firewall Enterprise S7032 hardware appliance

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.

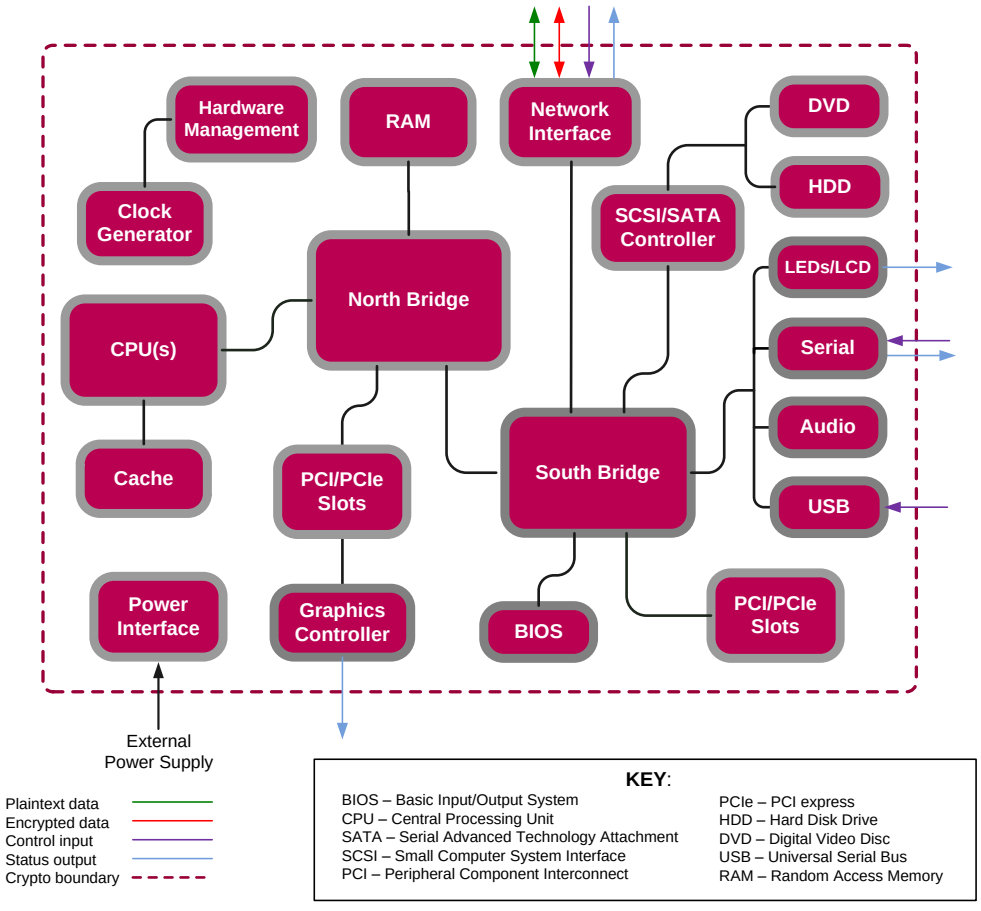

Figure 2 – Block Diagram of a Typical GPC

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, RAM[6], 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) consists of the McAfee Firewall Enterprise application, three cryptographic libraries, and a proprietary operating system (McAfee's SecureOS® v8.2) acting as the guest OS. The libraries are:

- Cryptographic Library for SecureOS (CLSOS) for 32-bit systems v7.0.1.01
- CLSOS for 64-bit systems v7.0.1.01
- Kernel Cryptographic Library for SecureOS (KCLSOS) v8.2

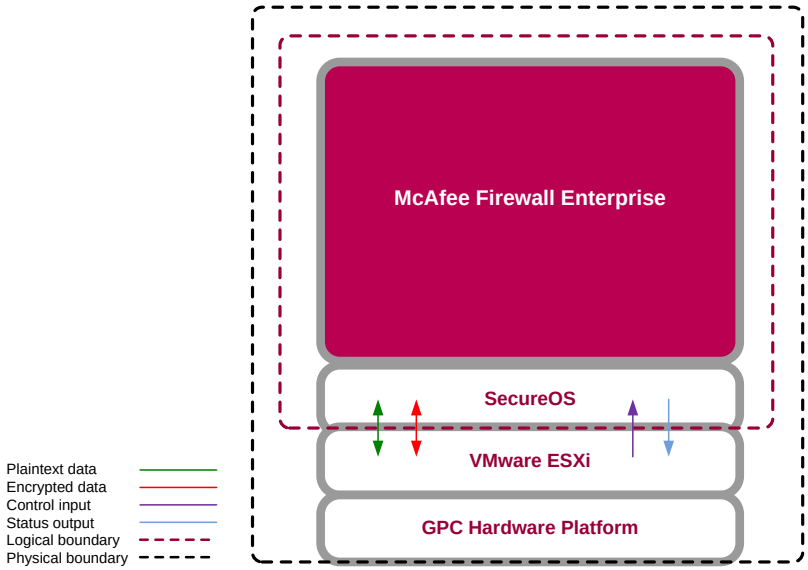

Figure 3 – MFE Virtual Appliance Cryptographic Boundaries

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

[6] RAM – Random Access Memory

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 2 below.

Table 2 – 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	• Data Input • Data Output • Control Input • Status Output
Host GPC Keyboard port	Virtual Keyboard port	• Control Input
Host GPC Mouse port	Virtual Mouse port	• Control Input
Host GPC Serial Port	Virtual Serial Port	• Data Input • Control Input
Host GPC Video Connector	Virtual Video Interface	• Status Output
Host GPC Power Interface	N/A	• 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

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

Please note that the keys and Critical Security Parameters (CSPs) listed in the Services tables below indicate 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

2.4.1 Crypto-Officer Role

The Crypto-Officer role performs administrative services on the module, such as initialization, configuration, and monitoring of the module. Before accessing the module for any administrative service, the operator must authenticate to the module. The module offers management interfaces in two ways:

- Administration Console
- Command Line Interface (CLI)

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 to the module are protected over secure TLS channel. Authentication of the administrator is through a username/password prompt checked against a local password database.

CLI sessions are offered by the module for troubleshooting. 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. The CO authenticates to the module using a username and password.

Services provided to the Crypto-Officer are provided in Table 3 below.

Table 3 – Crypto-Officer Services

Service	Description	Input	Output	CSP and Type of Access
Authenticate to the Admin Console	Used when administrators login to the appliance using the Firewall Enterprise Admin Console	Command	Status Output	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrative Password - R
Authenticate to the Admin Console using Common Access Card (CAC)	Used when administrators login to the appliance with CAC authentication to access the Firewall Enterprise Admin Console	Command	Status Output	Common Access Card Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Common Access Card One-Time Password - R
Authenticate to the Admin CLI	Used when administrators login to the appliance using the Firewall Enterprise Admin CLI	Command	Status Output	Firewall Authentication Keys - R Key Agreement Key - R SSH Session Authentication Key - R/W SSH Session Key - R/W Administrative Password - R
Authenticate to the Admin CLI using Common Access Card (CAC)	Used when administrators login to the appliance with CAC authentication to access the Firewall Enterprise Admin CLI	Command	Status Output	Common Access Card Authentication Keys - R Key Agreement Key - R SSH Session Authentication Key - R/W SSH Session Key - R/W Common Access Card One-Time Password - R
Authenticate to the local console	Used when administrators login to the appliance via the local console	Command	Status Output	Administrator Password - R
Change password	Allows external users to use a browser to change their Firewall Enterprise, SafeWord PremierAccess, or LDAP login password	Command	Status Output	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrative Password - R/W

Service	Description	Input	Output	CSP and Type of Access
Configure cluster communication	Services required to communicate with each other in Firewall Enterprise multi-appliance configurations	Command	Status Output	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure and monitor Virtual Private Network (VPN) services	Used to generate and exchange keys for VPN sessions	Command	Status Output	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	Create and monitor IPsec policy table that governs alternating bypass mode	Command	Status Output	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage mail services	Used when running 'sendmail' service on a Firewall Enterprise appliance	Command	Status Output	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	Command	Status Output	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	Command	Status Output	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	Command	Status Output	None
Enable FIPS mode	Configures the module in FIPS mode	Command	Status Output	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	Command	Status Output	None

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroizes the module to the factory default state	None	None	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

2.4.2 User Role

Users employ the services of the modules for establishing VPN[7] or TLS connections via Ethernet port. Access to these services requires the operator to first authenticate to the module. Descriptions of the services available to the Users are provided in Table 4 below.

Table 4 – User Services

Service	Description	Input	Output	CSP and Type of Access
Establish an authenticated TLS connection	Establish a TLS connection (requires operator authentication)	Command	Secure TLS session established	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	Command	Secure VPN tunnel established	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 Network User Role

The Network User role is defined as users within the secured network who have been given access to the device by a security policy rule granted by the Crypto-Officer. Network users communicate via plaintext connections (bypass). The Network User role does not require authentication.

Table 5 lists all the services that are available to the Network User role.

Table 5 – Network User Services

Service	Description	Input	Output	CSP and Type of Access
Establish a plaintext connection	Establish a plaintext connection	Command	Traffic in plaintext	None

2.4.4 Authentication Mechanism

While the module implements authentication mechanisms, there are no claims made regarding the authentication mechanisms meeting FIPS requirements beyond Level 1. However, the module employs the authentication methods described in Table 6 to authenticate Crypto-Officers and Users.

[7] VPN – Virtual Private Network

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, Certificate, or IP Address	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[8]/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is $1:2^{80}$, or $1:120,893 \times 10^{24}$. 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 VMware ESXi v4.1 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 the following operational environment and hardware:

- Intel Xeon processor running VMware ESXi v4.1 with McAfee's SecureOS v8.2 as the guest OS
- McAfee Firewall Enterprise S7032 appliance

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

[8] IKE – Internet Key Exchange

2.7 Cryptographic Key Management

The module implements three software cryptographic libraries to offer secure networking protocols and cryptographic functionalities. The software libraries for MFE v8.2.1 are:

- CLSOS Version 7.0.1.01 for 32-bit systems
- CLSOS Version 7.0.1.01 for 64-bit systems
- KCLSOS Version 8.2

Security functions offered by the libraries in FIPS mode of operation (and their associated algorithm implementation certificate numbers) are listed in Table 7.

Table 7 – Approved Security Functions

Approved Security Function	CLSOS 64-bit	CLSOS 32-bit	KCLSOS
Symmetric Key			
Advanced Encryption Standard (AES) 128/192/256-bit in CBC[9], ECB[10], OFB[11], CFB128[12] modes	1962	1961	-
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	1274	1273	-
Triple-DES 2- and 3-key options in CBC mode	-	-	1275
Asymmetric Key			
RSA[13] PKCS[14] #1 sign/verify: 1024/1536/2048/3072/4096-bit	1016	1015	-
RSA ANSI X9.31 key generation: 1024/1536/2048/3072/4096-bit	1016	1015	-
Digital Signature Algorithm (DSA) signature verification: 1024-bit	627	626	-
Secure Hash Standard			
SHA[15]-1, SHA-256, SHA-384, and SHA-512	1721	1720	1722
Message Authentication			
HMAC[16] using SHA-1, SHA-256, SHA-384, and SHA-512	1183	1182	1184
Random Number Generators (RNG)			
ANSI[17] X9.31 Appendix A.2.4 PRNG	1031	1030	1032

***NOTE**: As of December 31, 2010, the following algorithms listed in the table above are considered "deprecated" or "legacy use". For details regarding algorithm deprecation, please refer to NIST Special Publication 800-131A.*

- *Encryption using 2-key Triple DES*
- *Random number generation using ANSI X9.31-1998*
- *Digital signature generation using SHA-1*
- *Digital signature verification using 1024-bit DSA*
- *Digital signature generation and verification using 1024-bit RSA*
- *HMAC generation and verification using key lengths less than 112 bits*

[9] CBC – Cipher-Block Chaining
[10] ECB – Electronic Codebook
[11] OFB – Output Feedback
[12] CFB128 – 128-bit Cipher Feedback
[13] RSA – Rivest, Shamir, and Adleman
[14] PKCS – Public Key Cryptography Standard
[15] SHA – Secure Hash Algorithm
[16] HMAC – (Keyed-)Hash Message Authentication Code
[17] ANSI – American National Standards Institute

Non-FIPS-Approved security functions offered by the libraries in FIPS mode of operation are listed in Table 8.

Table 8 – Non-Approved Security Functions Used in FIPS Mode

Security Function	CLSOS 64-bit	CLSOS 32-bit	KCLSOS
Diffie-Hellman (DH): 1024/2048 bits[18] (key agreement)	implemented	implemented	-
RSA encrypt/decrypt[19] (key transport): 1024/1536/2048/3072/4096-bit	implemented	implemented	-
RNG (used to seed the KCLSOS PRNG)	-	-	-

***NOTE**: As of December 31, 2010, the following algorithms listed in the table above are considered "deprecated". For details regarding algorithm deprecation, please refer to NIST Special Publication 800-131A.*

- *1024-bit Diffie-Hellman key agreement*
- *1024-bit RSA key transport*

[18] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)
[19] Caveat: RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength)

.

The module supports the CSPs listed below in Table 9.

Table 9 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Session Key (v7.0.1.03 only)	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 1024/2048-bit keys or DSA 1024/2048-bit keys	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/private keys	RSA 1024/2048/4096-bit keys or DSA 1024-bit keys	Internally generated or imported electronically in plaintext via local management port	Encrypted form via network port or 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
Peer public keys	RSA 1024/2048/4096-bit keys or DSA 1024-bit keys	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[20] public/private keys	RSA 1024/2048/4096-bit keys or DSA 1024-bit keys	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
Key Establishment keys	Diffie-Hellman 1024/2048-bit keys, RSA 1024/1536/2048/3072/4096 -bit keys	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 TLS, IKE/IPsec and SSH sessions

[20] CA – Certificate Authority

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
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	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for TLS 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	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	- 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
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	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Data encryption/decryption for IPsec sessions

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IPsec Preshared Session Key	Triple-DES, AES-128, AES-256	- 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	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 Passwords	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
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
32-bit CLSOS X9.31 PRNG seed	16 bytes of seed value	Internally generated by KCLSOS ANSI X9.31 PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
32-bit CLSOS ANSI X9.31 PRNG key	AES-256	Internally generated by KCLSOS ANSI X9.31 PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
64-bit CLSOS ANSI X9.31 PRNG seed	16 bytes of seed value	Internally generated by KCLSOS ANSI X9.31 PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
64-bit CLSOS ANSI X9.31 PRNG key	AES-256	Internally generated by KCLSOS ANSI X9.31 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 by non-Approved RNG	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	Internally generated by non-Approved RNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
SSL CA key	RSA 1024/2048-bit key or DSA 1024/2048-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 1024/2048-bit key or DSA 1024/2048-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

The MFE Virtual Appliance performs the following self-tests at power-up:

- Software integrity check using HMAC SHA-256
- Cryptographic algorithm tests
  - AES Known Answer Test (KAT)
  - Triple-DES KAT
  - 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
  - RSA KAT for sign/verify and encrypt/decrypt
  - DSA pairwise consistency check
  - ANSI X9.31 Appendix A.2.4 PRNG KAT for all implementations

If any of the tests listed above fails to perform successfully, the module enters into a critical error state where all cryptographic operations and output of any data is prohibited. 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 ESXi v4.1 performs the following conditional self-tests:

- Continuous RNG Test (CRNGT) for all ANSI X9.31 implementations
- RSA pairwise consistency test upon generation of an RSA keypair
- DSA pairwise consistency test upon generation of an DSA keypair
- Manual key entry test
- Bypass test using SHA-1
- Software Load Test using DSA signature verification

Failure of the Bypass test or the CRNGT on the applicable KCLSOS PRNG 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.

2.8.3 Critical Functions Self-Test

The McAfee Firewall Enterprise Virtual Appliance for VMware ESXi v4.1 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 VMware ESXi v4.1 meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

Caveat: This guide assumes 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 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.

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 and install Firewall Enterprise version 8.2.1 for VMware ESXi 4.1, 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. Click **View Available Downloads**, and then click the link for the latest version.
   d. Click **I Agree** to accept the license agreement.
   e. Download the virtual image .zip file.
2. Download the product guide and release notes for the downloaded software version.
   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 version 8.2.1 installation guide.
3. Import the firewall
   a. Extract the .zip file you downloaded.
   b. Connect to your ESXi server using the VMware vSphere Client.
   c. From the menu bar, select **File | Deploy OVF Template**. The Deploy OVF Template window appears.
   d. 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.
   e. Click **Next**. The Name and Location page appears.
   f. Type a name for the firewall, and then click **Next**.
      - If the Ready to Complete page appears, proceed to Step i.
      - If the Network Mapping page appears, proceed to Step h.
      - If the Disk Format page appears, proceed to Step g.
        NOTE: This page appears only for ESXi 4.1 server.
   g. [For ESXi 4.1 server only] Select a format to store the virtual disks. You can select thin or thick provisioned format. Click **Next.**
   h. [Conditional] On the Network Mapping page, verify that **unconfigured** is selected in the **Destination Networks** drop-down list, then click **Next**. The Ready to Complete page appears.
   i. 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.

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. Installation and configuration instructions for the module can also be found in the *Secure Firewall Setup Guide*, *Secure Firewall Administration Guide*, and this FIPS 140-2 Security Policy. 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.

The Crypto-Officer must set FIPS mode enforcement to ensure that the module is running in its FIPS-Approved mode of operation.

3.1.2.1 Setting FIPS Mode Enforcement

Before enforcing FIPS on the module, the Admin Console CO must check that no non-FIPS-Approved service is running on the module. To view the services that are currently used in enabled rules, select "**Monitor / Service Status**". The Service Status window appears as shown in Figure 4 below. If the window lists any non-FIPS-Approved protocols (such as telnet as shown below), then those protocols must be disabled before the module is considered to be in its Approved mode of operation.

.

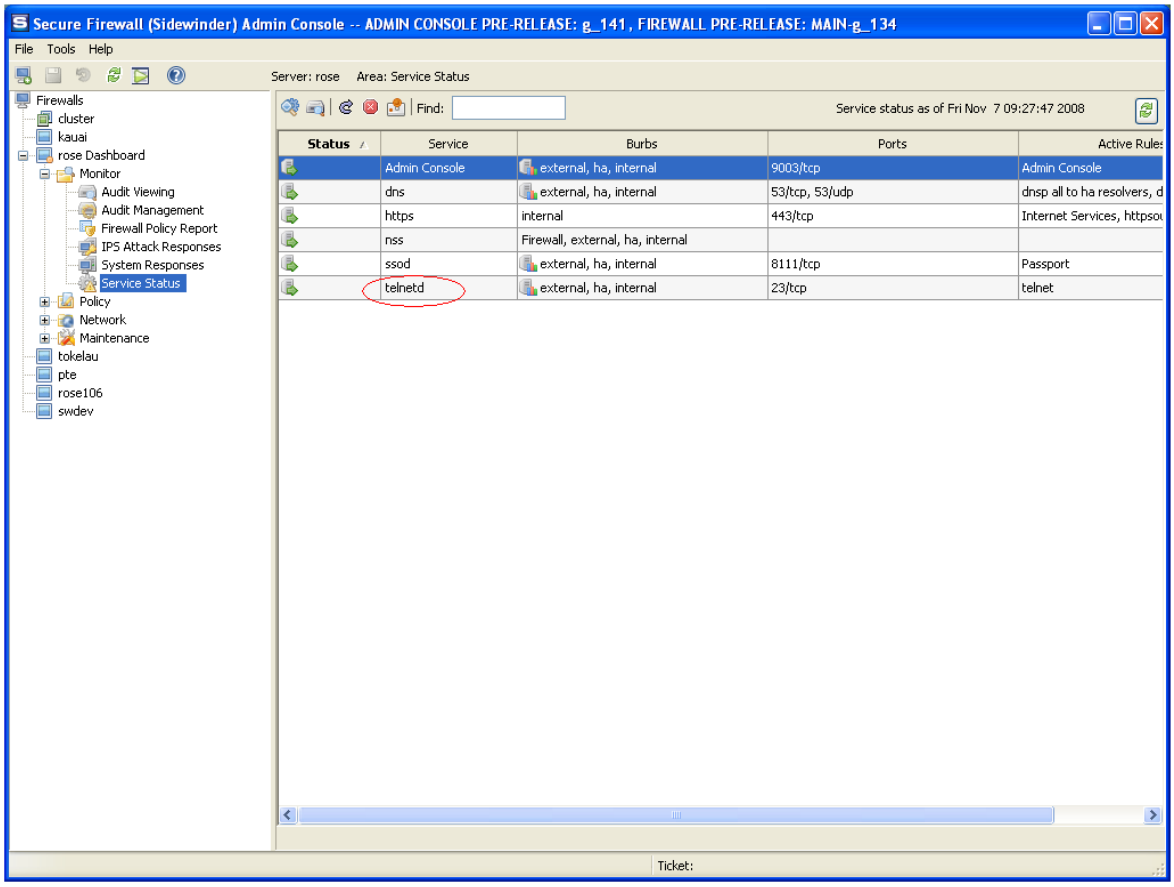

Figure 4 – Service Status

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 5).
4. Select "**Enforce U.S. Federal Information Processing Standard**".
5. Save the configuration change.
6. Select "**Maintenance / System Shutdown**" to reboot the firewall to the Operational kernel to activate the change.

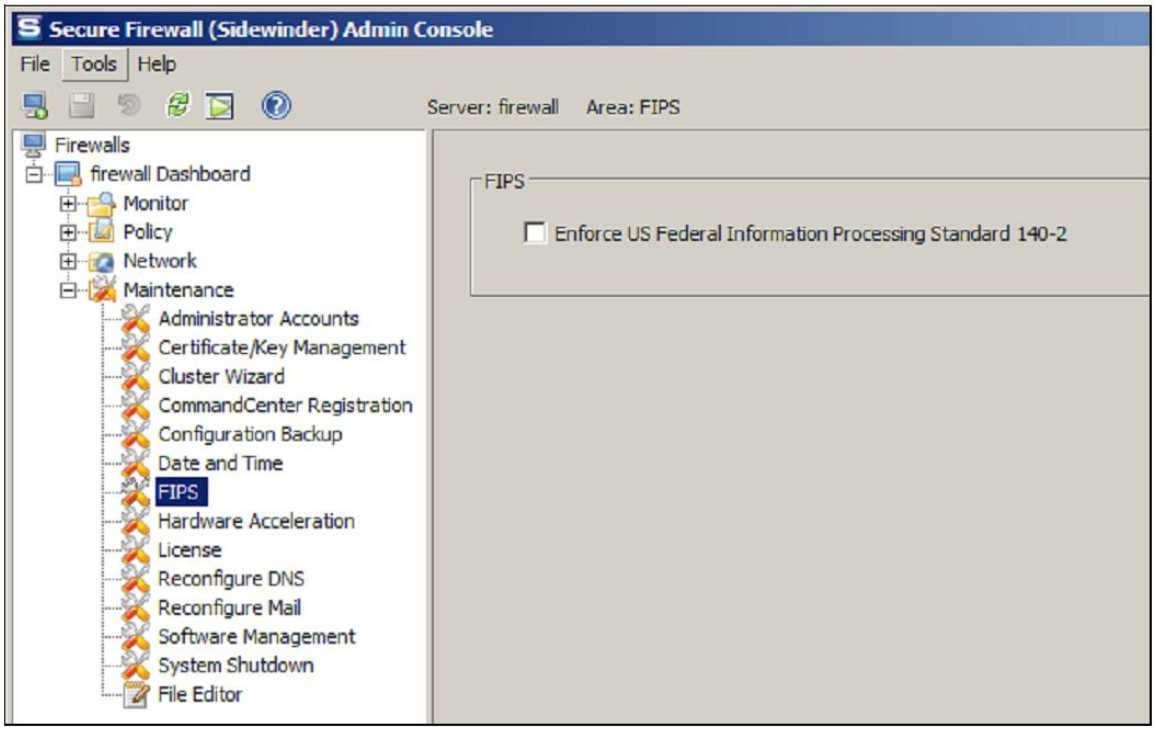

Figure 5 – Configuring For FIPS

The Crypto-Officer is required to delete and recreate all required cryptographic keys and CSPs necessary for the module's secure operation (please refer to Section 4 of the *McAfee Firewall Enterprise 8.2.0 FIPS 140-2 Configuration Guide* for details regarding the CSP update process). The keys and CSPs existing on the module were generated outside of FIPS mode of operation, and they must now be re-created for use in FIPS mode. The CO must replace the keys and CSPs listed in Table 10.

Table 10 – Required Keys and CSPs for Secure Operation

Services	Cryptographic Keys/CSPs
Admin Console (TLS)	Firewall Certificate/private key
Control Center (TLS)	Firewall Certificate/private key
HTTPS[21] 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

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

[21] HTTPS – Hypertext Transfer Protocol Secure

3.1.3 Management

Once configured to operate in FIPS-Approved mode, only FIPS-Approved and Allowed algorithms may be used. Non-FIPS-Approved services are disabled in FIPS mode of operation. 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 Secure Firewall Administration Guide. The Crypto-Officer should monitor the module's status regularly for active bypass mode. The CO also monitor that only FIPS-Approved algorithms as listed in Table 7 are being used for TLS and SSH sessions.

3.1.3.1 Status Indicators

The "show status" for FIPS mode of operation can be invoked by determining if the checkbox, shown in Figure 5, is checked. This can also be done via the CLI using the "**cf fips query**" command.

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 q type=bypass**" 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; the rebuild must be performed by McAfee. Once a factory reset has been performed, default keys and CSPs will be set up as part of the renewal process. These keys must be recreated as per the instructions found in Table 10. Failure to recreate these keys will result in a non-compliant module.

For more information about resetting the module to a factory default, please consult the documentation that shipped with the module.

3.2 User Guidance

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

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
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
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
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

.

Acronym	Definition
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
MD	Message Digest
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
RC	Rivest Cipher
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
USB	Universal Serial Bus
UTM	Unified Threat Management
VGA	Video Graphics Array
VPN	Virtual Private Network

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

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