McAfee, Inc.

McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032

Hardware Part Numbers: FWE-S1104, FWE-S2008, FWE-S3008, FWE-S4016, FWE-S5032, and FWE-S6032
Firmware Version: 8.3.2 with patch number 8.3.2E14

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
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

Table of Figures

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

List of Tables

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 Appliances from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 (Hardware Part Numbers: FWE-S1104, FWE-S2008, FWE-S3008, FWE-S4016, FWE-S5032, and FWE-S6032; Firmware Version: 8.3.2 with patch number 8.3.2E14) meet 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 appliances in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the appliances. The McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 Appliances are referred to in this document collectively as the MFE S-Series, 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.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 MFE S-Series Appliances

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. The MFE S-Series are 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.

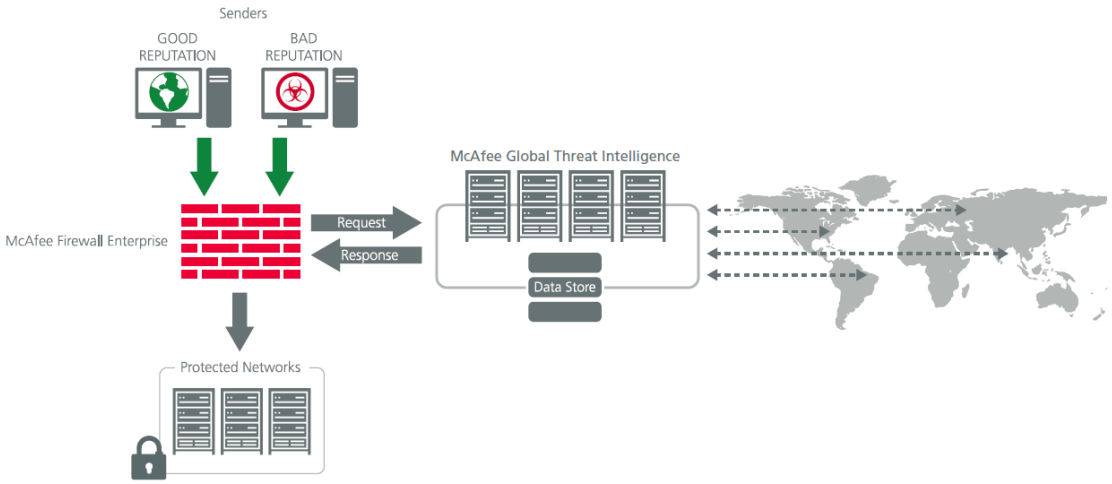


Figure 1 – Typical Deployment Scenario

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:

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

The MFE S-Series are 1U and 2U rack-mountable appliances. All of these appliances are appropriate for mid- to large-sized organizations. The appliances are shown in the figures below.

Figure 2 – McAfee MFE S1104

Figure 3 – McAfee MFE S2008

Figure 4 – McAfee MFE S3008

[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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 5 – McAfee MFE S4016

Figure 6 – McAfee MFE S5032/S6032

The MFE S-Series 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 S-Series 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 MIB[6], 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 mange their firewall solutions from the network edge to the core. Management communications between the MFE and Control Center are secured over a TLS session.

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

[6] MIB – Management Information Base

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The MFE S-Series 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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC[7]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The MFE S-Series is a multi-chip standalone hardware module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the MFE S-Series is defined by the hard metal chassis, which surrounds all the hardware and firmware components.

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

- McAfee Firewall Enterprise 32-bit Cryptographic Engine v8.3.2
- McAfee Firewall Enterprise 64-bit Cryptographic Engine 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.

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

[7] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[8] CBC – Cipher-Block Chaining
[9] ECB – Electronic Codebook
[10] OFB – Output Feedback
[11] CFB128 – 128-bit Cipher Feedback
[12] CTR – Counter

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Approved Security Function	Certificate #		
	32-Bit	64-Bit	KCLSOS
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	#1407	#1409	-
RSA[13] PKCS[14] #1 signature generation: 2048/3072-bit	#1407	#1409	-
RSA PKCS #1 signature verification: 1024/1536/2048/3072/4096-bit	#1407	#1409	-
DSA[15] PQG generation: 2048-bit	#828	#830	-
DSA PQG verification: 1024/2048/3072-bit	#828	#830	-
DSA key generation: 2048/3072-bit	#828	#830	-
DSA signature generation: 2048/3072-bit	#828	#830	-
DSA signature verification: 1024/2048/3072-bit	#828	#830	-
ECDSA[16] key generation (2048-bit); signature generation/verification (2048/256-bit)	#472	#474	-
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)			
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 DES[23]*

[13] RSA – Rivest, Shamir, and Adleman
[14] PKCS – Public Key Cryptography Standard
[15] DSA – Digital Signature Algorithm
[16] ECDSA – Elliptic Curve DSA
[17] SHA – Secure Hash Algorithm
[18] HMAC – (Keyed-) Hash Message Authentication Code
[19] ANSI – American National Standards Institute
[20] DRBG – Deterministic Random Bit Generator
[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)

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- *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 CVL[24] 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	-
Internet Key Exchange (IKE) v1 and v2	#168	-
Simple Network Management Protocol (SNMP) v3	-	#171

2.3 Module Interfaces

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

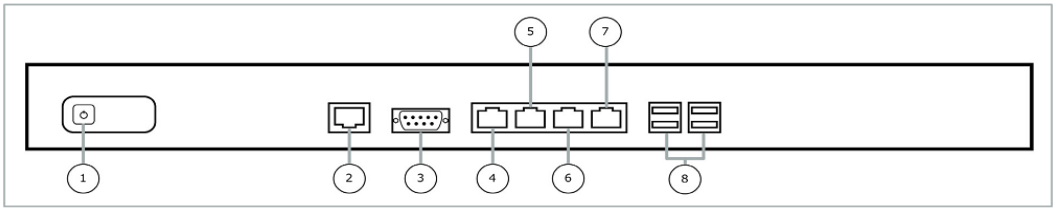
- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

[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 2^{20} plaintext data (or plaintext keys).
[24] CVL – Component Validation List

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

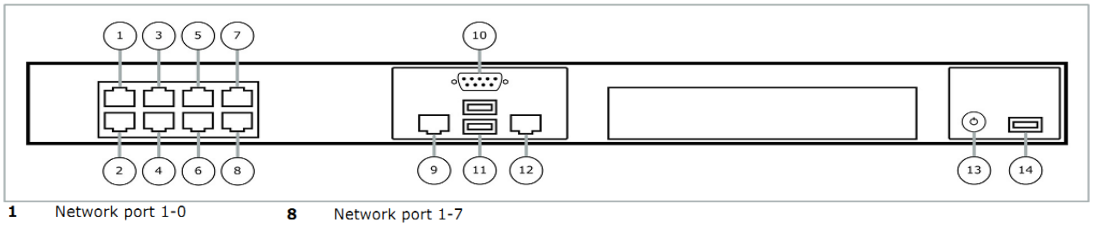
The physical ports and interfaces for the MFE S-Series appliances are depicted in Figure 7, Figure 8, Figure 9, Figure 10, and Figure 11. Note the following acronyms used in the figures below:

- RAID – Redundant Array of Independent Disks
- USB – Universal Serial Bus
- VGA – Video Graphics Array



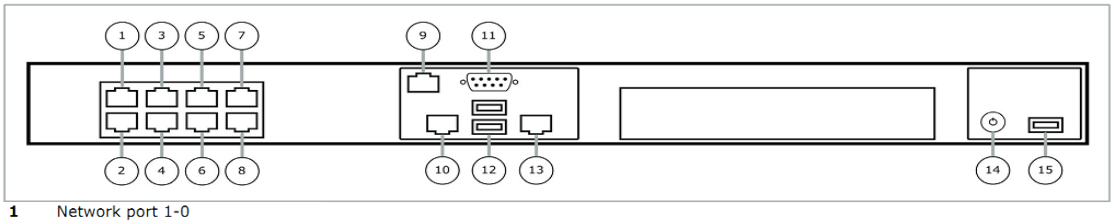
1	Power button	**5**	Network port 1-1
2	RS-232 serial port	**6**	Network port 1-2
3	VGA port	**7**	Network port 1-3
4	Network port 1-0	**8**	USB ports

Figure 7 – Front Panel Features and Indicators for S1104



1	Network port 1-0	**8**	Network port 1-7
2	Network port 1-1	**9**	Dedicated management port
3	Network port 1-2	**10**	VGA port
4	Network port 1-3	**11**	USB ports
5	Network port 1-4	**12**	RS-232 serial port
6	Network port 1-5	**13**	Power button
7	Network port 1-6	**14**	USB port

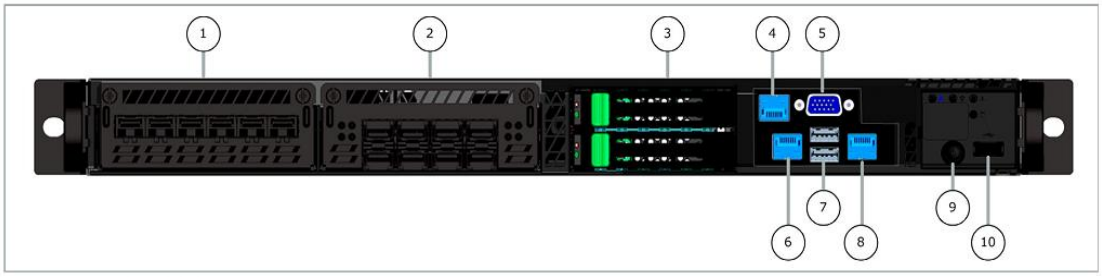
Figure 8 – Front Panel Features and Indicators for S2008



1	Network port 1-0	**9**	Remote Management Module port
2	Network port 1-1	**10**	Dedicated management port mgr1
3	Network port 1-2	**11**	VGA port
4	Network port 1-3	**12**	USB ports
5	Network port 1-4	**13**	RS-232 serial port
6	Network port 1-5	**14**	Power button
7	Network port 1-6	**15**	USB port
8	Network port 1-7		

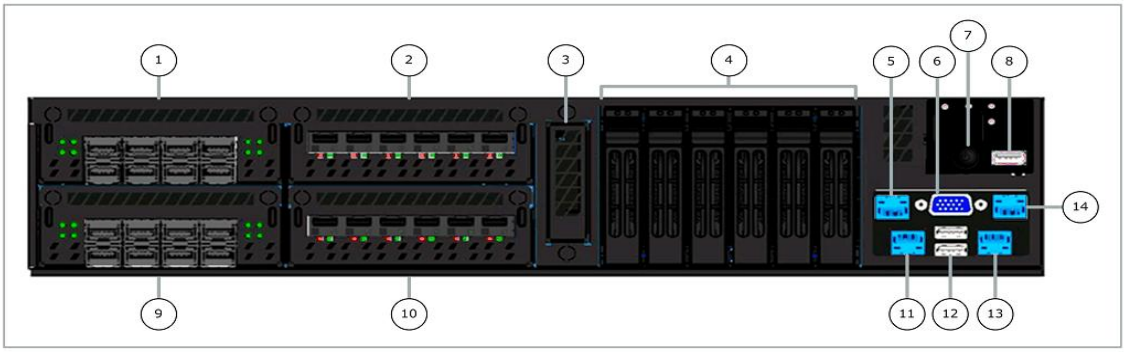
Figure 9 – Front Panel Features and Indicators for S3008

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.



1	Network module bay 1	**6**	Dedicated management port
2	Network module bay 2	**7**	USB ports
3	Hard drive bays	**8**	RS-232 serial port
4	Remote Management Module Ethernet port	**9**	Power button
5	VGA port	**10**	USB port

Figure 10 – Front Panel Features and Indicators for S4016



1	Network module bay 1	**8**	USB port
2	Network module bay 3	**9**	Network module bay 2
3	RAID battery module	**10**	Network module bay 4
4	Hard drive bays	**11**	Dedicated management port 1
5	Remote Management Module Ethernet port	**12**	USB ports
6	VGA port	**13**	RS-232 serial port
7	Power button	**14**	Dedicated management port 2

Figure 11 – Front Panel Features and Indicators for S5032 and S6032

***NOTE**: The Remote Management Module ports that appear on the S4016, S5032, and S6032 appliances (see Figure 10 and Figure 11) are not operational in the MFE deployments.*

The back panels of McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 contain power connectors. LEDs[25] are located on the front control panels of MFE S-Series and can be used for quick hardware diagnostics. There are two LEDs on S1104, four LEDs on S2008, S3008, and S4016, and five LEDs on S5032 and S6032. The two LEDs on the S1104 are shown in Figure 2; Figure 12 and Figure 13 show the control panels for the other appliances.

[25] LED – Light Emitting Diode

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

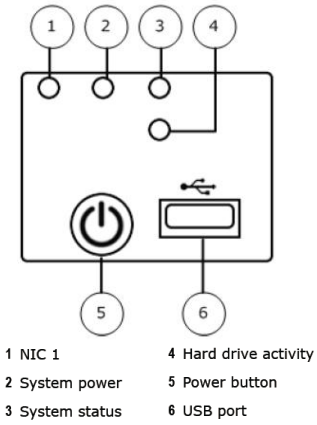


Figure 12 – S2008, S3008, and S4016 Control Panel

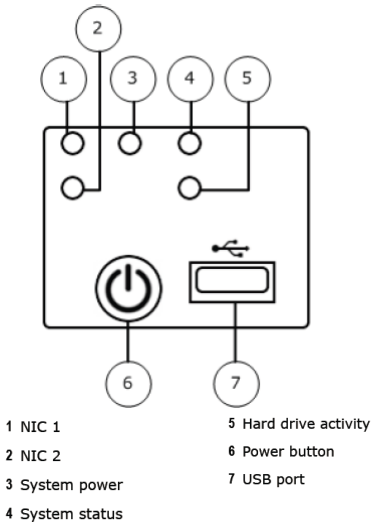


Figure 13 – S5032 and S6032 Control Panel

The behaviors of the LEDs are as shown in Table 4, Table 5, Table 6, and Table 7.

Table 4 – Behavior of Network Activity LEDs

Network Activity LEDs (S2008, S3008, S4016, S5032, S6032)		
Color	**State**	**Description**
Green	On	NIC Link/no access
	Blink	LAN[26] access

Table 5 – Behavior of Power LED

[26] LAN – Local Area Network

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Power LED (S1104, S2008, S3008, S4016, S5032, S6032)		
Color	**State**	**Description**
Green	On	Power On
	Blink	Sleep / ACPI[27] S1 state
Off	Off	Power Off / ACPI S4 state

Table 6 – Behavior of System Status LED

System Status LED (S2008, S3008, S4016, S5032, S6032)			
Color	**State**	**Criticality**	**Description**
Green	Solid on	System OK	System booted and ready
	Blink	Degraded	System degraded: - Non-critical temperature threshold asserted - Non-critical voltage threshold asserted - Non-critical fan threshold asserted - Fan redundancy lost, sufficient system cooling maintained (this does not apply to non-redundant systems) - Power supply predictive failure - Power supply redundancy lost (this does not apply to non-redundant systems)
Amber	Blink	Non-critical	Non-fatal alarm – system is likely to fail: - Critical temperature threshold asserted - Critical voltage threshold asserted - Critical fan threshold asserted
	Solid on	Critical, non-recoverable	Fatal alarm – system has failed or shut down: - CPU[28] Missing - Thermal Trip asserted - Non-recoverable temperature threshold asserted - Non-recoverable voltage threshold asserted - Power fault/Power Control Failure - Fan redundancy lost, insufficient system cooling (this does not apply to non-redundant systems) - Power supply redundancy lost insufficient system power (this does not apply to non-redundant systems) **Note: This state also occurs when AC power is first applied to the system. This indicates the BMC[29] is booting.**

[27] ACPI – Advanced Configuration and Power Interface
[28] CPU – Central Processing Unit
[29] BMC – Baseboard Management Controller

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

System Status LED (S2008, S3008, S4016, S5032, S6032)			
Color	**State**	**Criticality**	**Description**
Off	N/A[30]	Not ready	- AC[31] power off, if no degraded, non-critical, critical, or non-recoverable conditions exist. - System is powered down or S5 states, if no degraded, non-critical, critical, or non-recoverable conditions exist.

Table 7 – Behavior of Drive Activity LED

Drive Activity LED (S1104, S2008, S3008, S4016, S5032, S6032)		
Color	**State**	**Description**
Green	Random Blink	HDD access
Off	Off	No hard disk activity

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 8.

Table 8 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Module Interface	
	S1104	S2008, S3008, S4016, S5032, S6032
Data Input	Connectors (Ethernet)	Connectors (Ethernet)
Data Output	Connectors (Ethernet)	Connectors (Ethernet)
Control Input	Connectors (Ethernet, USB, serial) and button (power)	Connectors (Ethernet, USB, serial) and button (power)
Status Output	Connectors (VGA, Ethernet, serial), and LED indicators (power-on, drive activity)	Connectors (VGA, Ethernet, serial), and LED indicators (power-on, drive activity, system status, network activity)
Power	Connectors (power)	Connectors (power)

2.4 Roles and Services

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

[30] N/A – Not Applicable
[31] AC – Alternating Current

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4.1 Authorized Roles

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

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

- User Role – Users employ the services of the modules for establishing VPN[32] 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 9 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 9 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

Table 9 – 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

[32] VPN – Virtual Private Network

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Role		CSP and Type of Access
		CO	User	
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
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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Role		CSP and Type of Access
		CO	User	
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
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
Configure the SNMP Agent	Configures the SNMP Agent for status monitoring of non-FIPS-relevant information	x		SNMP v3 Session Key - R

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Role		CSP and Type of Access
		CO	User	
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
Load package	Downloads available firmware update or patch	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
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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4.3 Authentication Mechanisms

The module 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 10 to authenticate Crypto-Officers and Users.

Table 10 – 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.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Role	Type of Authentication	Authentication Strength
User	Password or Certificate	Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is $1:94^8$, or 1: 6,095,689,385,410,816. This would require about 60,956,893,854 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding. Certificates used as part of TLS, SSH, and IKE[33]/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is $1:2^{80}$, or $1:1.20893 \times 10^{24}$. 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 $1:2^{128} \times 94^8$.

2.5 Physical Security

The MFE S-Series is a multi-chip standalone cryptographic module. The module is contained in a hard metal chassis which is defined as the cryptographic boundary of the module. The module's chassis is opaque within the visible spectrum. The enclosure of the module has been designed to satisfy Level 2 physical security requirements. Tamper-evident seals are applied to the case to provide physical evidence of attempts to remove the chassis cover or front bezel. Additionally, the tamper-evident seals must be inspected periodically for tamper evidence. The placement of the tamper-evident seals can be found in Secure Operation section of this document.

The MFE S-Series has been tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.6 Operational Environment

The requirements in this section are not applicable, as the module does not provide a general-purpose operating system (OS) to module operators. McAfee's proprietary SecureOS version 8.3 provides a limited

[33] IKE – Internet Key Exchange

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

operational environment, and only the module's custom-written image can be run on the OS. The module provides a method to update the firmware in the module with a new version. This method involves downloading a digitally-signed firmware update to the module.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 11.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Table 11 – 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[34] 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

[34] CA – Certificate Authority

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

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)

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

At power-up, the MFE S-Series automatically performs a firmware 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 12 (note that the table indicates the library with which each test is associated).

Table 12 – 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 S1104, S2008, S3008, S4016, S5032, and S6032 conducts conditional cryptographic algorithm self-tests as indicated in Table 13 (again, note that the table indicates the library with which each test is associated).

Table 13 – 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	✓	-

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

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

Failure of the Bypass test or the KCLSOS PRNG CRNGT 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 2 requirements for this validation.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Secure Operation

The MFE S-Series meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in its Approved mode of operation. The use of any interfaces and services not documented herein are prohibited and considered in violation of this Security Policy, and shall result in the non-compliant operation of the module.

3.1 Crypto-Officer Guidance

The Crypto-Officer will receive the module from the vendor via trusted delivery services (UPS, FedEx, etc.). The Crypto-Officer shall ensure that the shipment contains the following:

- MFE S-Series appliance
- Media and Documents
- Activation Certificate
- Setup Guide
- Port Identification Guide
- Management Tools CD[35]
- Firewall Enterprise Installation Media USB drive (for appliances without a CD-ROM[36] drive)
- Power cord
- Rack mount kit

For appliance setup, the Crypto-Officer receives a FIPS Kit separately, also via trusted delivery service. The FIPS Kit (part number FRU-686-0089-00) includes the FIPS Kit instructions, a new warranty seal, and tamper-evident seals.

The Crypto-Officer is responsible for the proper initial setup of the Admin Console Management Tool software and the cryptographic module. Setup of the Admin Console software is done by installing the software on an appropriate Windows® workstation (refer to the *McAfee Firewall Enterprise version 8.3.0 Product Guide* for details regarding installation of management tools) on the same network as the module. When you install the Admin Console, 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 Appliance Setup

Before the module can be placed into its Approved mode of operation, the Crypto-Officer shall install all required physical security mechanisms.

3.1.1.1 Applying Tamper-Evident Seals

The CO must place tamper-evident seals on the module as described in the information provided below. After the seals are placed as instructed below, the module can be powered up and the Crypto-Officer may proceed with initial configuration.

3.1.1.1.1 Prepare Module for Tamper-Evident Seal Application

[35] CD – Compact Disc
[36] CD-ROM – Compact Disc - Read-Only Memory

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

To apply the seals, the appliance surfaces and front bezel must first be cleaned with isopropyl alcohol in the area where the tamper-evident seals will be placed. Prior to affixing the seals, the front bezel must be attached.

3.1.1.1.2 S1104 Tamper-Evident Seal Application

The S1104 has a removable top panel, held in place by two screws at the rear of the appliance. This panel must be secured by placing two (2) tamper-evident seals on the appliance as indicated in red in Figure 14, where:

1: Rear of appliance
2: Tamper-evident seal
3: Screws
4: Tamper-evident seal

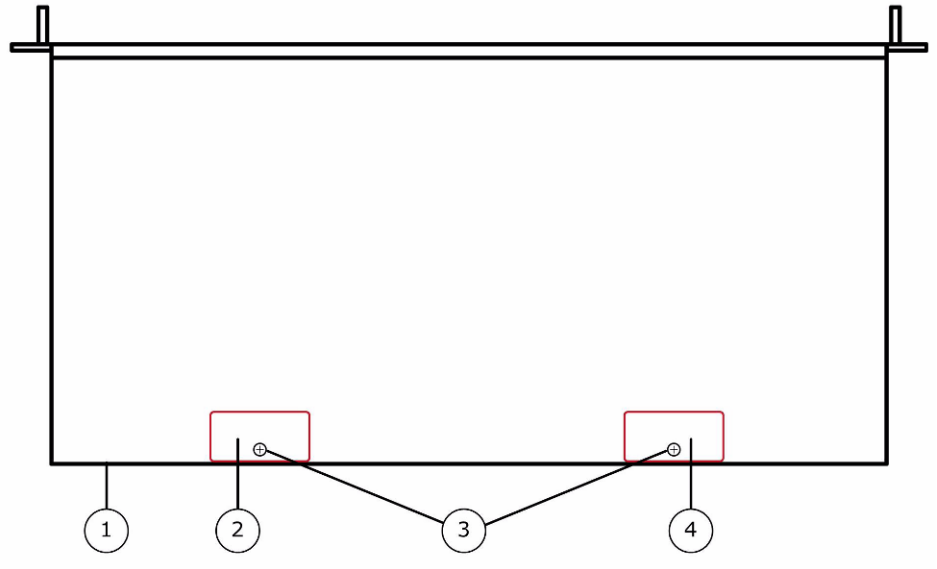


Figure 14 – Tamper-Evident Seal Application Positions (S1104)

3.1.1.1.3 S2008 / 3008 Tamper-Evident Seal Application

The S2008 and S3008 each have a removable top panel that must be secured. Place one (1) tamper-evident seal on the top cover as indicated in red in Figure 15, where:

1: Front of appliance
2: Tamper-evident seal

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Figure 15 – Tamper-Evident Seal Application Positions (S2008 / S3008)

3.1.1.1.4 S4016 Tamper-Evident Seal Application

The S4016 has removable top panels and power supplies that must be secured. Place four (4) tamper-evident seals on the appliance as indicated in red in Figure 16.

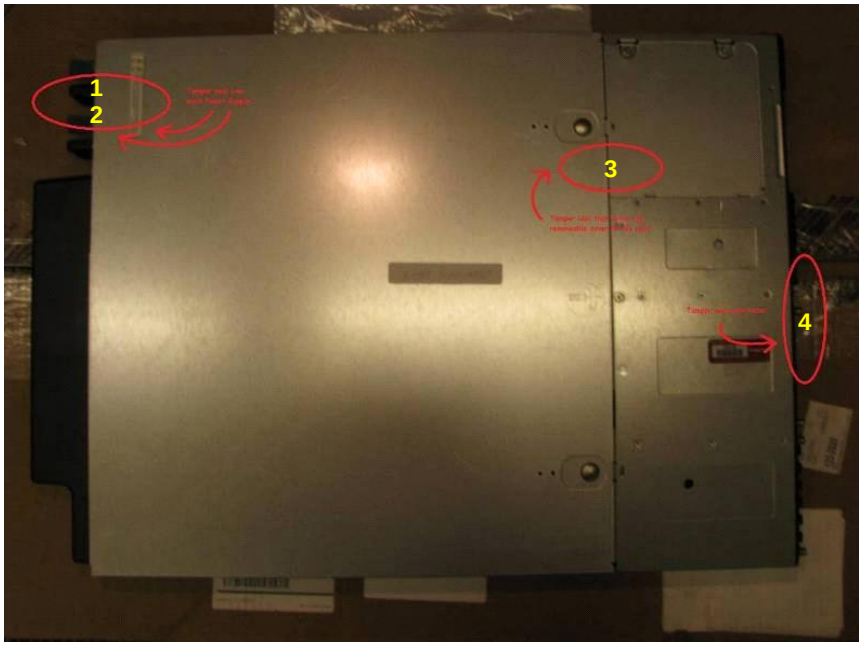


Figure 16 – Tamper-Evident Seal Application Positions (S4016)

3.1.1.1.5 S5032 / S6032 Tamper-Evident Seal Application

The S5032 and S6032 each have a removable cover and power supplies that must be secured. Place thirteen (13) tamper-evident seals on the appliance as indicated in yellow in Figure 17, Figure 18, Figure 19, and Figure 20.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

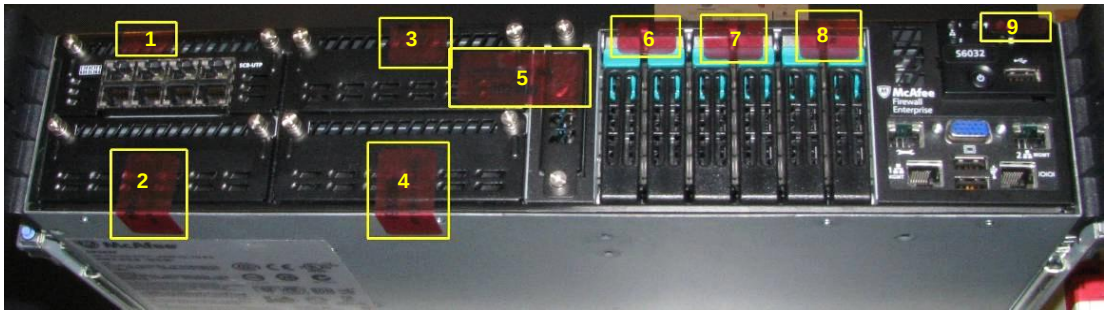


Figure 17 – Tamper-Evident Seal Application Positions (S5032 / S6032 – Front)

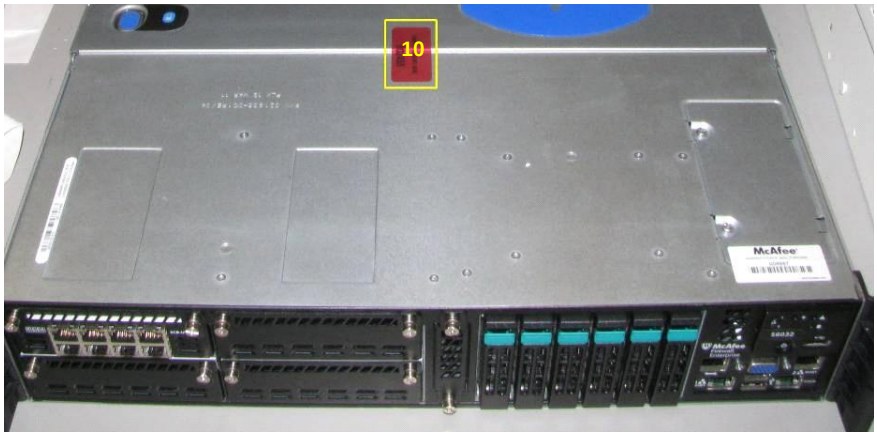


Figure 18 – Tamper-Evident Seal Application Position (S5032 / S6032 – Top)

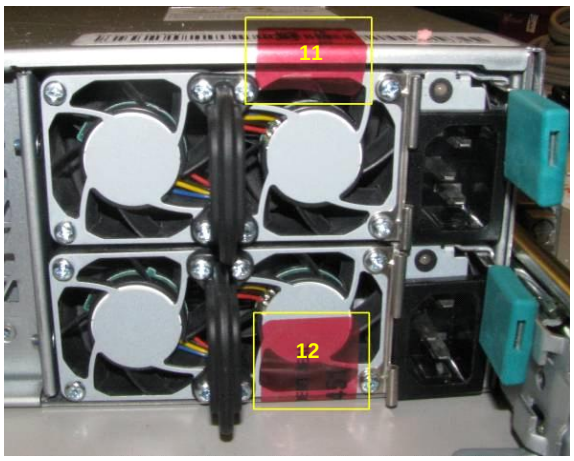


Figure 19 – Tamper-Evident Seal Application Positions (S5032 / S6032 – Rear)

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 20 – Tamper-Evident Seal Application Positions (S5032 / S6032 – Bottom Rear)

3.1.2 Installation

The cryptographic module requires that proper firmware version (including baseline version and patch code) be installed on the appliance. As part of installation, the Crypto-Officer must perform the following activities:

- Modify the BIOS[37]
- Install the module firmware

3.1.2.1 Modifying the BIOS

Enter the module's System Setup program to enforce the following module usage policies:

- Booting the module from any device other than the FIPS-enabled hard drive is prohibited.
- Only authenticated users are allowed to enter the System Setup program.

Additionally, since the module's power button is not accessible, the AC Power Recovery setting must be modified. Follow the instructions below to update the BIOS settings (requires the connection of a monitor and keyboard):

S1104 BIOS Settings

1. From the command line, restart the firewall.
2. When *Press <DEL> or <F2> to enter setup* appears in the upper right corner of the screen, press the <F2> key. The BIOS window appears.
3. Load the optimized default settings.
   a. Press <F3>.
   b. At the prompt, select **Yes**, and then press <Enter>.
4. Configure a BIOS password to prevent the firewall from booting from other devices.
   a. Use the arrow keys to select the **Security** menu.
   b. Select **Administrator Password**, and then press <Enter>.
   c. Enter a password and a confirmation, and then press <Enter>.
5. Set the power restore option.
   a. Use the arrow keys to select the **Chipset** menu.
   b. Select **Southbridge**, and then press <Enter>.
   c. Select **Restore AC Power Loss**, and then press <Enter>.
   d. Select **Power On**, and then press <Enter>.
6. Save changes and exit the BIOS.
   a. Press <F4>.
   b. The firewall will then complete its startup process.

S2008 / S3008 / S4016 / S5032 / S6032 BIOS Settings

[37] BIOS – Basic Input/Output System

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

1. From the command line, restart the firewall.
2. When *Press <DEL> or <F2> to enter setup* appears in the upper right corner of the screen, press the <F2> key. The BIOS window appears.
3. Load the optimized default settings.
   a. Press <F9>.
   b. At the prompt, select **Yes**, and then press <Enter>.
4. Configure a BIOS password to prevent the firewall from booting from other devices.
   a. Use the arrow keys to select the **Security** menu.
   b. Select **Set Administrator Password**, and then press <Enter>.
   c. Enter a password and a confirmation, and then press <Enter>.
5. Set the power restore option.
   a. Use the arrow keys to select the **Server Management** menu.
   b. Select **Resume on AC Power Loss**, and then press <Enter>.
   c. Select **Reset**, and then press <Enter>.
6. Save changes and exit the BIOS.
   a. Press <F10>.
   b. At the prompt, select **Yes**, and then press <Enter>.
   c. The firewall will then complete its startup process.

3.1.2.2 Installing the Module Firmware

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 Firewall Enterprise version 8.3.2, 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 installation USB image (.zip).
6. Write the image to a USB drive.

To install the firmware image onto the appliance, the Crypto-Officer must:

1. Insert the USB drive and start/restart the firewall.
2. Enter the boot menu, and then select the installation USB drive. The firewall boots from the installation media.
3. At the **McAfee Inc.** menu, accept the default, which is the **Operational System**.
4. At the **Welcome to McAfee Firewall Enterprise** menu, select the appropriate Firewall Enterprise boot option.
5. When the installation complete message appears, remove the installation media from the firewall.
6. Press "**R**" to restart the firewall, and then press "**Enter**". The firewall restarts and displays standard restart information.

Version 8.3.2 is now installed on the appliance. 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**.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

3.1.3 Initialization

The Crypto-Officer is responsible for initialization and security-relevant configuration and management activities for the module. Initialization and configuration instructions for the module can also be found in the *McAfee Firewall Enterprise version 8.3.x Quick Start Guide*, *McAfee Firewall Enterprise version 8.3.2 Product 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.

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 21 below. From here, select the "**Active Rules**" button in the upper right corner of the window (see Figure 22). 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.

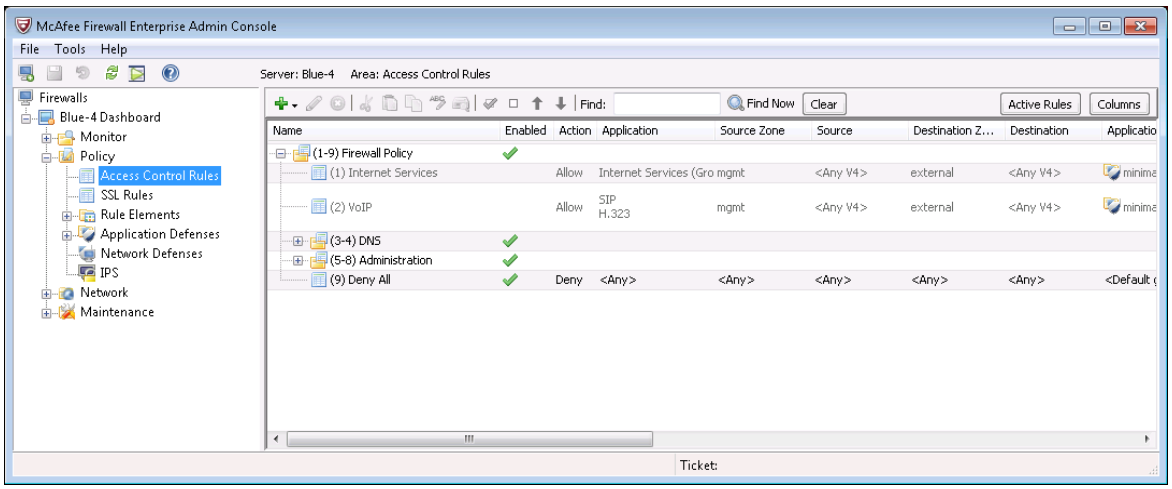


Figure 21 – Rules Window

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

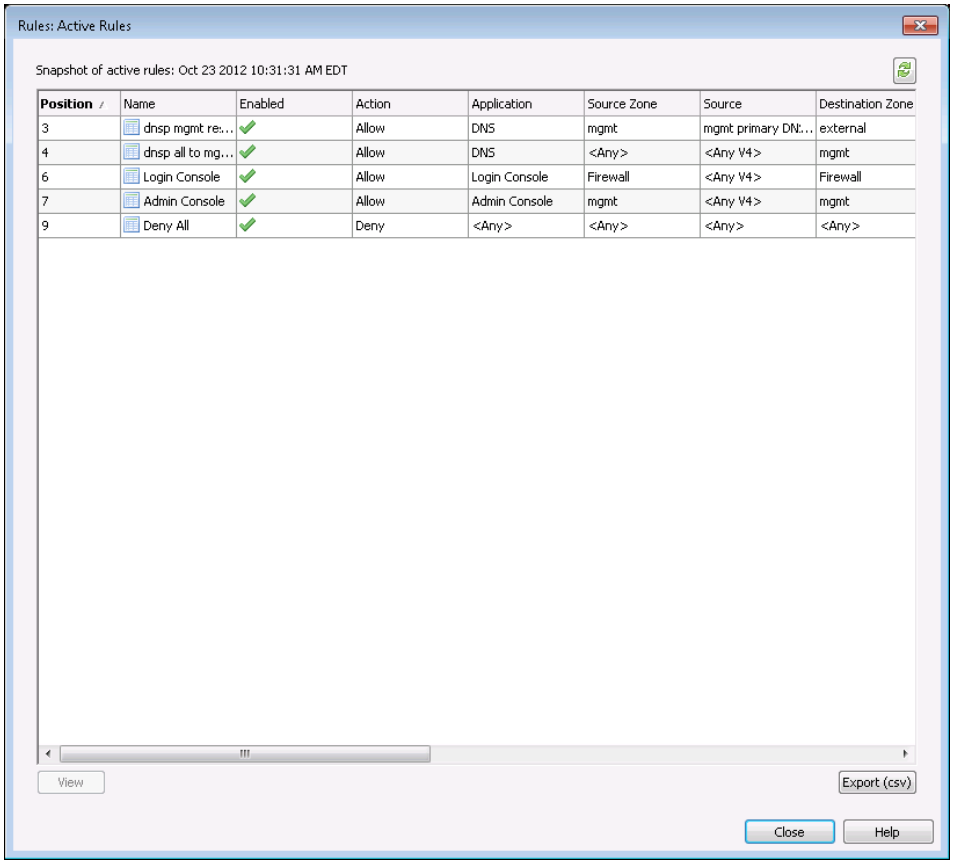


Figure 22 – Active Rules Window

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 Approved cryptographic algorithms.
3. Select "**Maintenance / FIPS**". The FIPS check box appears in the right pane (shown in Figure 23).
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.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

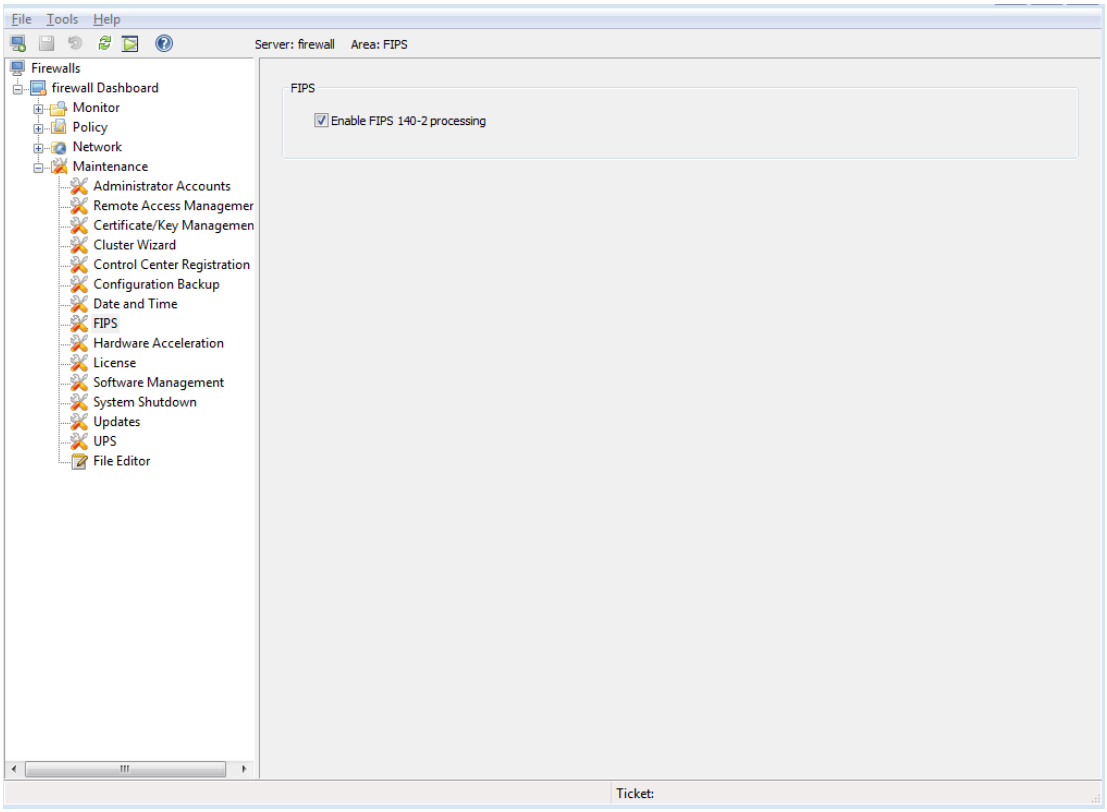


Figure 23 – Configuring For FIPS

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.

3.1.4 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 above 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 Service should be contacted.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.1.5 Physical Inspection

For the module to operate in its Approved mode, the tamper-evident seals must be placed by the CO role as specified in Section 3.1.1 above. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO is also responsible for the following:

- securing and having control at all times of any unused seals
- direct control and observation of any changes to the module where the tamper-evident seals are removed or installed to ensure that the security of the module is maintained during such changes and that the module is returned to its Approved state

The CO is also required to periodically inspect the module for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of malice. If evidence of tampering is found during periodic inspection, the Crypto-Officer must return the module to McAfee for key zeroization and re-imaging before the module can be brought back into operation.

To request additional seals, the Crypto-Officer can contact McAfee Customer Service via email at service@mcafee.com. The Crypto-Officer must be sure to include contact information and the shipping address, as well as the appliance serial number.

3.1.6 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 23. 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.

3.1.7 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 **Error! Reference source not found.**. 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.

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Acronyms

This section describes the acronyms used throughout the document.

Table 14 – Acronyms

Acronym	Definition
AC	Alternating Current
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
CAC	Common Access Card
CAST	Carlisle Adams and Stafford Tavares
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
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CVL	Component Validation List
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Acronym	Definition
EMI	Electromagnetic Interference
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
IG	Implementation Guidance
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
KAT	Known Answer Test
KCLSOS	Kernel Cryptographic Library for SecureOS
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
MD	Message Digest
MFE	McAfee Firewall Enterprise
MIB	Management Interface Base
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMS	Network Management System
OFB	Output Feedback
OS	Operating System
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Acronym	Definition
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

© 2014 McAfee, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

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

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