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 Versions: 7.0.1.03 and 8.2.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: **2**
Document Version: **0.6**

Prepared for:

McAfee, Inc.
3965 Freedom Circle
Santa Clara, California 95054
United States of America

Phone: +1 (888) 847-8766

Prepared by:

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

Phone: +1 (703) 267-6050

Prepared for:
http://www.mcafee.com

Prepared by:
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 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 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 Appliances, 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 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. McAfee Firewall Enterprise appliances 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, 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.

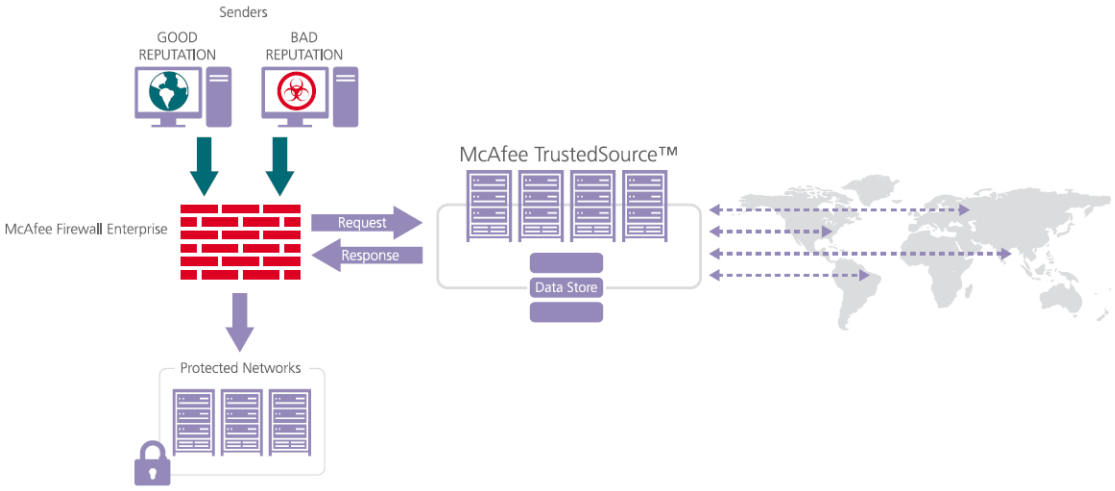


Figure 1 – Typical Deployment Scenario

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

Although SNMP v3 can support AES encryption, it does not utilize a FIPS-Approved key generation method; therefore, the module has been designed to block the ability to view or alter critical security parameters (CSPs) through this interface. Also note that the SNMP v3 interface is a management interface for the MFE S-Series Appliances and that no CSPs or user data are transmitted over this interface.

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

Figure 2 – McAfee Firewall Enterprise S1104 (Front and Rear View)

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

Figure 3 – McAfee Firewall Enterprise S2008 (Front and Rear View)

Figure 4 – McAfee Firewall Enterprise S3008 (Front and Rear View)

Figure 5 – McAfee Firewall Enterprise S4016 (Front and Rear View)

Figure 6 – McAfee Firewall Enterprise S5032/S6032 (Front and Rear View)

The McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 appliances are 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[5]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The MFE S-Series Appliances (Hardware Part Numbers: FWE-S1104, FWE-S2008, FWE-S3008, FWE-S4016, FWE-S5032, and FWE-S6032; Firmware Versions: 7.0.1.03 and 8.2.0) are multi-chip standalone hardware modules that meet overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the MFE S-Series Appliances is defined by the hard metal chassis, which surrounds all the hardware and firmware components.

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

2.3 Module Interfaces

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

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

The physical ports and interfaces for the model MFE S-Series Appliances are listed in Table 2, and are depicted in Figure 7, Figure 8, Figure 9, Figure 10, and Figure 11.

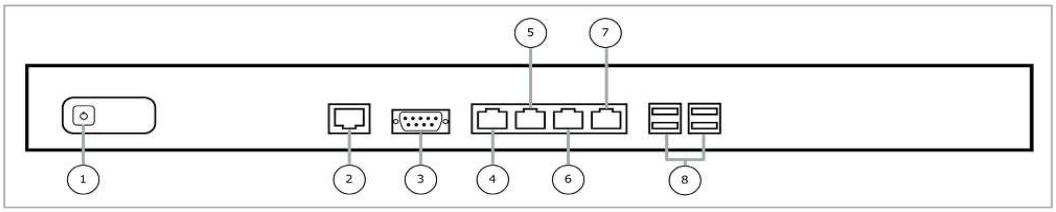
Table 2 – MFE S-Series Appliances Ports and Interfaces

Location	Physical Port/Interface	S1104	S2008	S3008	S4016	S5032	S6032
Front Panel	Ethernet RJ-45 Port	4	9	10	18	35	35
	USB[6] Port	4	3	3	3	3	3
	Serial Port	1	1	1	1	1	1
	VGA[7] Port	1	1	1	1	1	1
	Power Button	1	1	1	1	1	1
	Power LED[8]	1	1	1	1	1	1
	Drive-Activity LED	1	1	1	1	1	1
	Status LED	0	1	1	1	1	1
	Network Activity LED	0	1	1	1	2	2
Back Panel	Power connector	1	1	1	2	2	2

With regard to the figures that follow, please note:

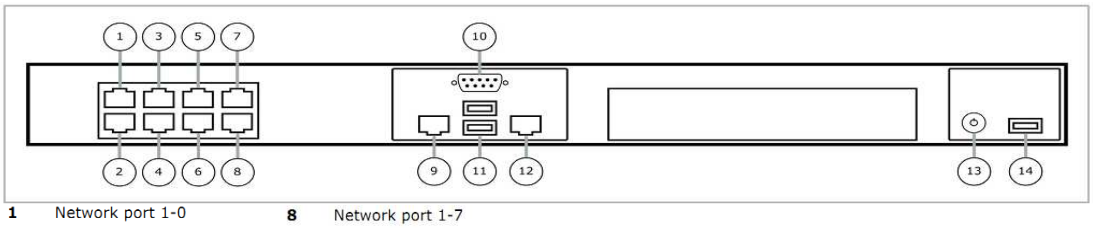
- The following conventions are used to label the network ports in the figures below:
  - Network module bay number where the Ethernet port is installed ("1" is used for appliances that do not have network module bays)
  - Ethernet port number (labeled on the network module)
  - This information is combined to create the NIC[9] name in the form of <*module bay number*>-<*Ethernet port number*>.

[6] USB – Universal Serial Bus
[7] VGA – Video Graphics Array
[8] LED – Light-Emitting Diode
[9] NIC – Network Interface Controller



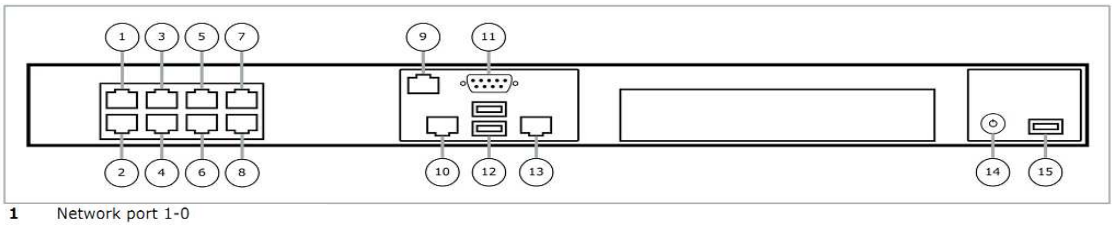
1	Power button	**5**	Network port 1-1
2	RS-232 serial port	**6**	Network port 1-2
3	VGA port	**7**	Network port 1-3
4	Network port 1-0	**8**	USB ports

Figure 7 – Front Panel Features and Indicators for S1104



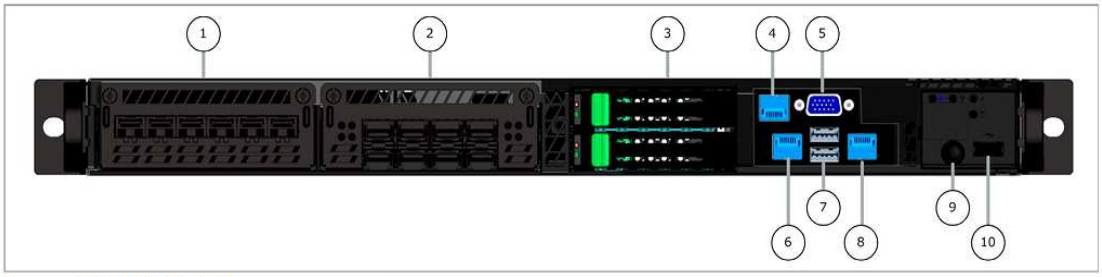
1	Network port 1-0	**8**	Network port 1-7
2	Network port 1-1	**9**	Dedicated management port
3	Network port 1-2	**10**	VGA port
4	Network port 1-3	**11**	USB ports
5	Network port 1-4	**12**	RS-232 serial port
6	Network port 1-5	**13**	Power button
7	Network port 1-6	**14**	USB port

Figure 8 – Front Panel Features and Indicators for S2008



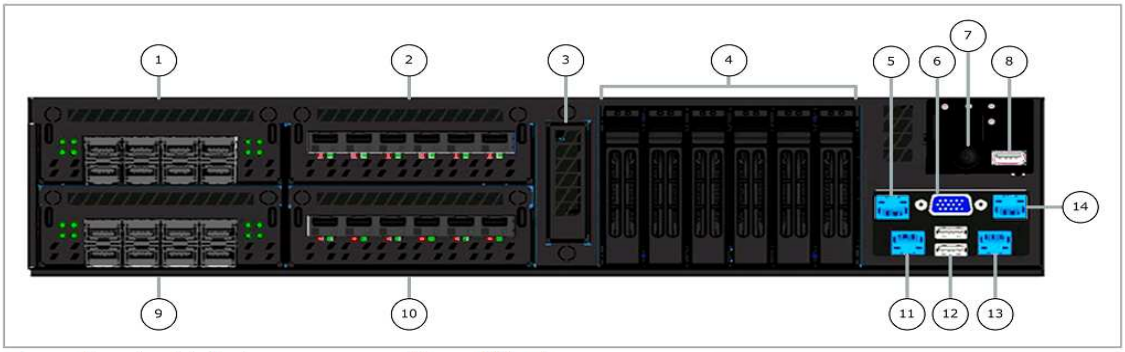
1	Network port 1-0	**9**	Remote Management Module port
2	Network port 1-1	**10**	Dedicated management port mgr1
3	Network port 1-2	**11**	VGA port
4	Network port 1-3	**12**	USB ports
5	Network port 1-4	**13**	RS-232 serial port
6	Network port 1-5	**14**	Power button
7	Network port 1-6	**15**	USB port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

Figure 9 – Front Panel Features and Indicators for S3008



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 as depicted in Figure 2 to Figure 8 and listed in Table 2.

The LEDs are located on the front panels of MFE S-Series Appliances 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 clearly visible in Figure 2 while the positions of the LEDs for other appliances are shown in Figure 12 and are as follows:

- The upper far left LED is the Network Activity LED for the management port 1.
- The lower far left LED is the Network Activity LED for the management port 2 (only on the S5032 and S6032).
- The middle LED is the Power LED.
- The upper far right LED is the Status LED.

- The lower far right LED is the Drive Activity LED.

Figure 12 – LED Indicators

The behaviors of the LEDs are as shown in Table 3, Table 4, Table 5, and Table 6.

Table 3 – Behavior of Network Activity LEDs

Network Activity LEDs (S2008, S3008, S4016, S5032, S6032)		
Color	**State**	**Description**
Green	On	NIC Link/no access
	Blink	LAN[10] access

Table 4 – Behavior of Power LED

Power LED (S1104, S2008, S3008, S4016, S5032, S6032)		
Color	**State**	**Description**
Green	On	Power On
	Blink	Sleep / ACPI[11] S1 state
Off	Off	Power Off / ACPI S4 state

Table 5 – Behavior of Status LED

Status LED (S2008, S3008, S4016, S5032, S6032)			
Color	**State**	**Criticality**	**Description**
Green	Solid	System OK	System booted and ready

[10] LAN – Local Area Network
[11] ACPI – Advanced Configuration and Power Interface

Status LED (S2008, S3008, S4016, S5032, S6032)			
Color	**State**	**Criticality**	**Description**
	on		
	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[12] 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[13] is booting.**
Off	N/A[14]	Not ready	- AC[15] 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.

[12] CPU – Central Processing Unit
[13] BMC – Baseboard Management Controller
[14] N/A – Not Applicable
[15] AC – Alternating Current

Table 6 – 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 7.

Table 7 – 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 module supports role-based 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 three ways:

- Administration Console
- Command Line Interface (CLI)
- SNMP v3

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.

The cryptographic module uses the SNMP v3 protocol for remote management, and to provide information about the state and statistics as part of a Network Management System (NMS).

Services provided to the Crypto-Officer are provided in Table 8 below.

Table 8 – 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 Public/Private 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 Public/Private Keys - R Key Agreement Key - R SSH Session Authentication Key - R/W SSH Session Key - R/W Administrative Password - R

Service	Description	Input	Output	CSP and Type of Access
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 Public/Private Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrative Password - R/W
Configure cluster communication	Services required to communicate with each other in Firewall Enterprise multi-appliance configurations	Command	Status Output	Firewall Authentication Public/Private 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 Public/Private 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 Public/Private 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 Public/Private Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	Input	Output	CSP and Type of Access
Manage web filter	Manages configuration with the SmartFilter	Command	Status Output	Firewall Authentication Public/Private 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 Public/Private Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Monitor status on SNMP	Monitors non security relevant status of the module via SNMPv3	Command	Status Output	SNMP v3 Session Key - R
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 Public/Private 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
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 (v8.2.0 only) - R/W SSL Server Certificate key (v8.2.0 only) - R/W

2.4.2 User Role

Users employ the services of the modules for establishing VPN[16] 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 Users are provided in the table below.

[16] VPN – Virtual Private Network

Table 9 – 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 Public/Private Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W SSL CA key (v8.2.0 only) - R SSL Server Certificate key (v8.2.0 only) - R
Establish a VPN connection	Establish a VPN connection over IPsec tunnel	Command	Secure VPN tunnel established	Firewall Authentication Public/Private 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 10 lists all the services that are available to the Network User role.

Table 10 – 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

The module employs the authentication methods described in Table 11 to authenticate Crypto-Officers and Users.

Table 11 – 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 × 10^6 × 60 seconds, or 6 x 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[17]/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is 1:2^{80}, or 1:120,893 x 10^{24}. The fastest network connection supported by the module is 1000 Mbps. Hence, at most 60,000,000,000 bits of data (1000 × 10^6 × 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} x 84^4.

2.5 Physical Security

The cryptographic module 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.

[17] IKE – Internet Key Exchange

The MFE S-Series Appliances have 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 operational environment requirements do not apply to the MFE S-Series Appliances, because the modules do not provide a general-purpose operating system (OS) to the user. The OS has limited operational environment and only the modules' custom written image can be run on the system. The modules provide 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 implements three firmware cryptographic libraries to offer secure networking protocols and cryptographic functionalities. The firmware libraries for MFE v7.0.1.03 are:

- Cryptographic Library for SecureOS® (CLSOS) Version 7.0.1.01 for 32-bit systems
- CLSOS Version 7.0.1.01 for 64-bit systems
- Kernel CLSOS (KCLSOS) Version 7.0.1.01

The firmware libraries for MFE v8.2 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 12.

Table 12 – Approved Security Functions

Approved Security Function	CLSOS 64-bit	CLSOS 32-bit	KCLSOS 7.0.1.01	KCLSOS 8.2
Symmetric Key				
Advanced Encryption Standard (AES) 128/192/256-bit in CBC[18], ECB[19], OFB[20], CFB128[21] modes	972	973	-	-
AES 128/192/256-bit in CBC, ECB modes	-	-	974	1833
Triple Data Encryption Standard (DES) 2- and 3-key options in CBC, ECB, OFB, CFB64 modes	765	766	-	-
Triple-DES 2- and 3-key options in CBC mode	-	-	767	1185
Asymmetric Key				

[18] CBC – Cipher-Block Chaining
[19] ECB – Electronic Codebook
[20] OFB – Output Feedback
[21] CFB128 – 128-bit Cipher Feedback

Approved Security Function	CLSOS 64-bit	CLSOS 32-bit	KCLSOS 7.0.1.01	KCLSOS 8.2
RSA[22] PKCS[23] #1 sign/verify: 1024/1536/2048/3072/4096-bit	469	470	-	-
RSA ANSI X9.31 key generation: 1024/1536/2048/3072/4096-bit	469	470	-	-
Digital Signature Algorithm (DSA) signature verification: 1024-bit	338	339	-	-
Secure Hash Standard				
SHA[24]-1, SHA-256, SHA-384, and SHA-512	941	942	943	1612
Message Authentication				
HMAC[25] using SHA-1, SHA-256, SHA-384, and SHA-512	544	545	546	1086
Random Number Generators (RNG)				
ANSI[26] X9.31 Appendix A.2.4 PRNG	549	550	551	964

***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.*

- *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/verification using 1024-bit RSA*
- *HMAC generation and verification using key lengths less than 112 bits*

Non-FIPS-Approved security functions offered by the libraries in FIPS mode of operation are listed in Table 13.

Table 13 – Non-Approved Security Functions Used in FIPS Mode

Security Function	CLSOS 64-bit	CLSOS 32-bit	KCLSOS 7.0.1.01	KCLSOS 8.2
Diffie-Hellman (DH): 1024/2048 bits[27] (key agreement)	implemented	implemented	-	-
RSA encrypt/decrypt[28] (key transport): 1024/1536/2048/3072/4096-bit	implemented	implemented	-	-

***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*

[22] RSA – Rivest, Shamir, and Adleman
[23] PKCS – Public Key Cryptography Standard
[24] SHA – Secure Hash Algorithm
[25] HMAC – (Keyed-)Hash Message Authentication Code
[26] ANSI – American National Standards Institute
[27] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)
[28] Caveat: RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength)

The module also implements the non-FIPS-Approved algorithms listed in Table 14 to be used in non-FIPS mode of operation.

Table 14 – Non-Approved Security Functions Used in Non-FIPS Mode

Security Function	CLSOS 64-bit	CLSOS 32-bit	KCLSOS 7.0.1.01	KCLSOS 8.2
Blowfish	implemented	implemented	-	-
Rivest Cipher (RC) 4	implemented	implemented	-	-
RC2	implemented	implemented	-	-
Message Digest (MD) 5	implemented	implemented	-	-
DES	implemented	implemented	-	-

The module supports the CSPs listed below in Table 15.

Table 15 – 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 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[29] 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

[29] CA – Certificate Authority

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
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
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

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	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	- 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

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
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
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 from entropy sources	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
KCLSOS ANSI X9.31 PRNG key	AES-256	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 (v8.2.0 only)	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 (v8.2.0 only)	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 S-Series Appliances perform the following self-tests at power-up:

- Firmware integrity check using SHA-1 Data Authentication Code (DAC)
- 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 S1104, S2008, S3008, S4016, S5032, and S6032 perform 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
- Firmware Load Test using DSA signature verification

Failure of the Bypass test or the CRNGT on the 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 Tests

The McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 perform the following critical functions 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 2 requirements for this validation.

3 Secure Operation

The McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, and S6032 meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-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 is responsible for initialization and security-relevant configuration and management of the module. Please see McAfee's Administration Guide for more information on configuring and maintaining the module. The Crypto-Officer receives the module from the vendor via trusted delivery services (UPS, FedEx, etc.). The shipment should contain the following:

- McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, or S6032 appliance
- Media and Documents
- Activation Certificate
- Setup Guide
- Port Identification Guide
- Management Tools CD[30]
- Secure Firewall Installation Media USB drive (for appliances without a CD-ROM[31] drive)
- Power cord
- Rack mount kit
- 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.

When you install the Management Tool, a link to the documents page is added to the "Start" menu of the computer. To view the Secure Firewall documents on the McAfee web site, select

Start > Programs > McAfee > Firewall Enterprise > Online Manuals

Table 16 provides a list of available Firewall Enterprise documents.

Table 16 – Summary of Firewall Enterprise Documentation

Document	Description
Secure Firewall Setup Guide	Leads through the initial firewall configuration.
Secure Firewall Administration Guide	Complete administration information on all firewall functions and features.
Secure Firewall Control Center Setup Guide	Leads through the initial Control Center configuration.

[30] CD – Compact Disc
[31] CD-ROM – Compact Disc – Read-Only Memory

Document	Description
Secure Firewall Control Center Administration Guide	Complete administration information on all Control Center functions and features. This guide is supplemented by the Secure Firewall Administration Guide.
Common Access Card Configuration Guide	Describes how to configure Department of Defense Common Access Card authentication for Admin Console, Telnet, and SSH on McAfee® Firewall Enterprise. It also describes login procedures.
Online help	Online help is built into Secure Firewall Management Tools programs. The Quick Start Wizard provides help for each configuration window. The Admin Console program provides help for each window, as well as comprehensive topic-based help. Note: A browser with a pop-up blocker turned on, must allow blocked content to view the Secure Firewall help.

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

3.1.1 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 perform five activities to ensure that the module is running in its FIPS-Approved mode of operation:

- Apply tamper-evident seals
- Modify the BIOS[32]
- Confirm the firmware version
- Set FIPS mode enforcement

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. 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. The seals must be placed as instructed before the module is powered up and the Crypto-Officer proceeds with initial configuration.

S1104 Seal Application and Placement

The S1104 module 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 13, where:

[32] BIOS – Basic Input/Output System

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

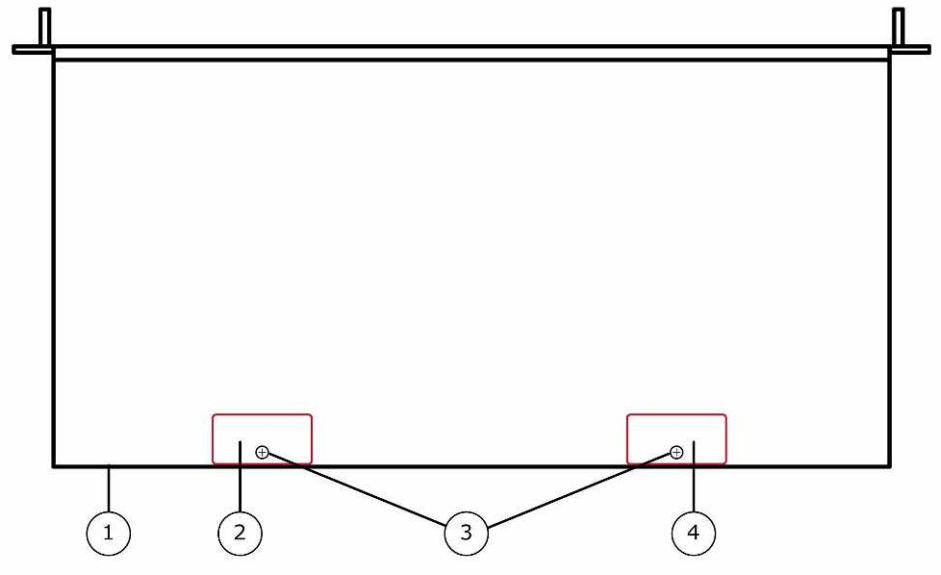


Figure 13 – Tamper-Evident Seal Application Positions (S1104)

S2008/S3008 Seal Application and Placement

The S2008 and S3008 module has a removable top panel that must be secured. Place one (1) tamper-evident seal on the top cover as indicated in red in Figure 14, where:

1: Front of appliance
2: Tamper-evident seal

Figure 14 – Tamper-Evident Seal Application Positions (S2008/S3008)

S4016 Seal Application and Placement

The S4016_module 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 15.

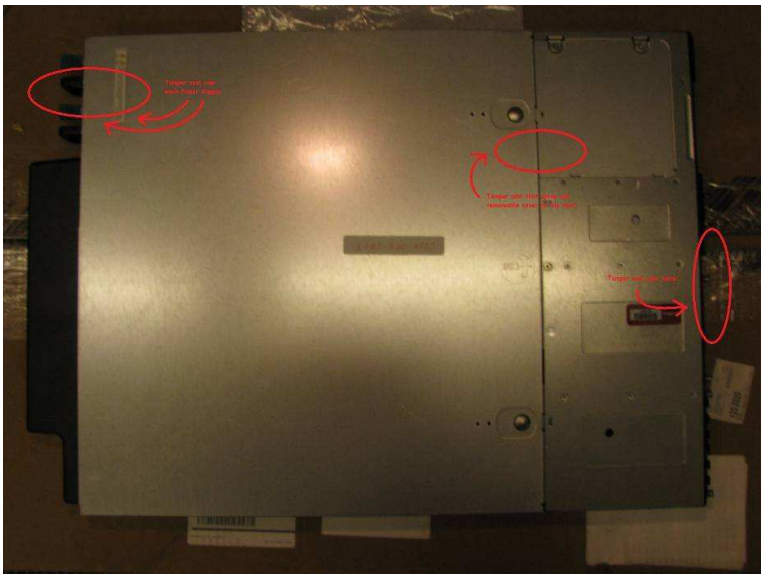


Figure 15 – Tamper-Evident Seal Application Positions (S4016)

S5032/S6032 Seal Application and Placement

The S5032 and S6032 modules have removable covers and power supplies that must be secured. Place thirteen (13) tamper-evident seals on the appliance as indicated in yellow in Figure 16, Figure 17, Figure 18, and Figure 19.

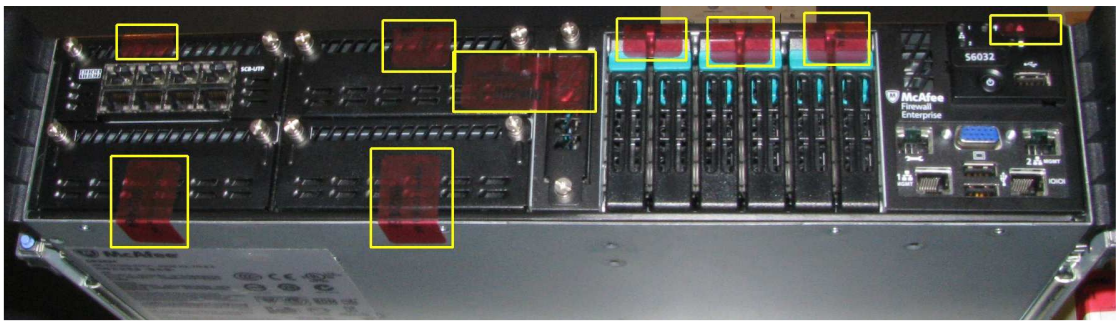


Figure 16 – Tamper-Evident Seal Application Positions (S5032/S6032 – Front)

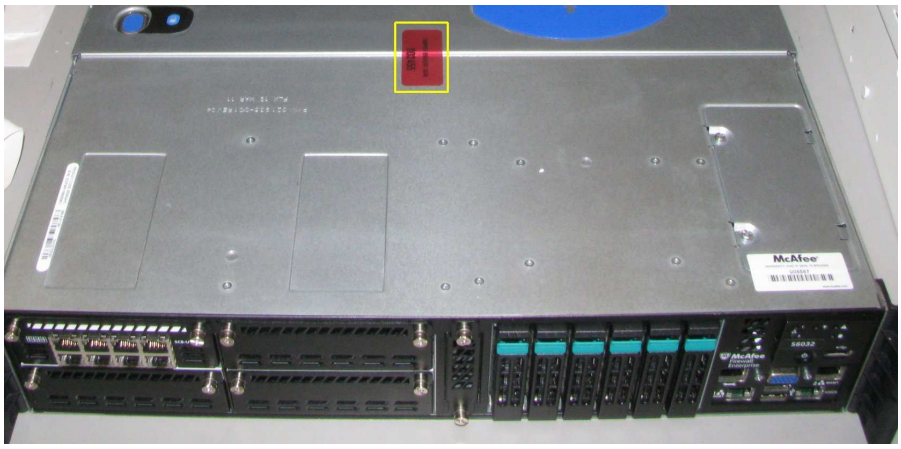


Figure 17 – Tamper-Evident Seal Application Position (S5032/S6032 – Top)

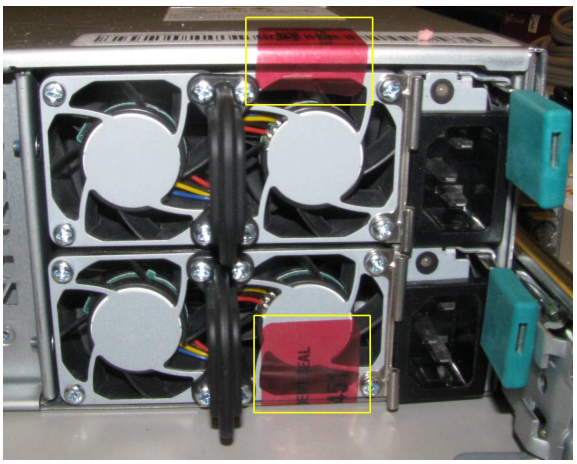


Figure 18 – Tamper-Evident Seal Application Positions (S5032/S6032 – Rear)

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

3.1.1.2 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 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 <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.

S4016/S5032/S6032 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 <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.

3.1.1.3 Confirming the Firmware Version

The cryptographic module requires that proper firmware version be installed. While some models may have the correct version pre-installed, others may require upgrading. To check if the module is currently running the correct version, the Crypto-Officer must open the GUI-based Admin Console provided with the module. Under the software management and manage packages table, the Crypto-Officer can see which firmware upgrade has been installed along with their versions. If the installed version requires to be upgraded to a validated version, please follow the steps below.

- Upgrading to 7.0.1.03

  To perform the upgrade to version **7.0.1.03**, the Crypto-Officer must first check the firmware to ensure they are running version **7.0.1.02**. If this version is not running, the Crypto-Officer must first take measures to upgrade the module to **7.0.1.02**. If required, this upgrade can be performed through Admin Console. If the module is being newly-built from the onboard virtual disk, then the Crypto-Officer will first need to set up the network configuration and enable the admin account with a new password.

  To upgrade from **7.0.1.02** to **7.0.1.03**, the Crypto-Officer must:

  1. Under "**Software Management / Manage Packages**" table, select "70103".
  2. Select download.
  3. Select install.
  4. Verify that the "**Manage Packages**" tab states that "70103" is installed.

- Upgrading to 8.2.0

  To perform the upgrade to version **8.2.0**, the Crypto-Officer must first check the firmware to ensure they are running version **8.1.2**. If this version is not running, the Crypto-Officer must first take measures to upgrade the module to **8.1.2**. If required, this upgrade can be performed through Admin Console. If the module is being newly-built from the onboard virtual disk, then the Crypto-Officer will first need to set up the network configuration and enable the admin account with a new password.

  To upgrade from **8.1.2** to **8.2.0**, the Crypto-Officer must:

  1. Under "**Software Management / Manage Packages**" table, select "8.2.0".
  2. Select download.
  3. Select install.
  4. Verify that the "**Manage Packages**" tab states that "8.2.0" is installed.

3.1.1.4 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 20 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 an approved FIPS mode of operation.

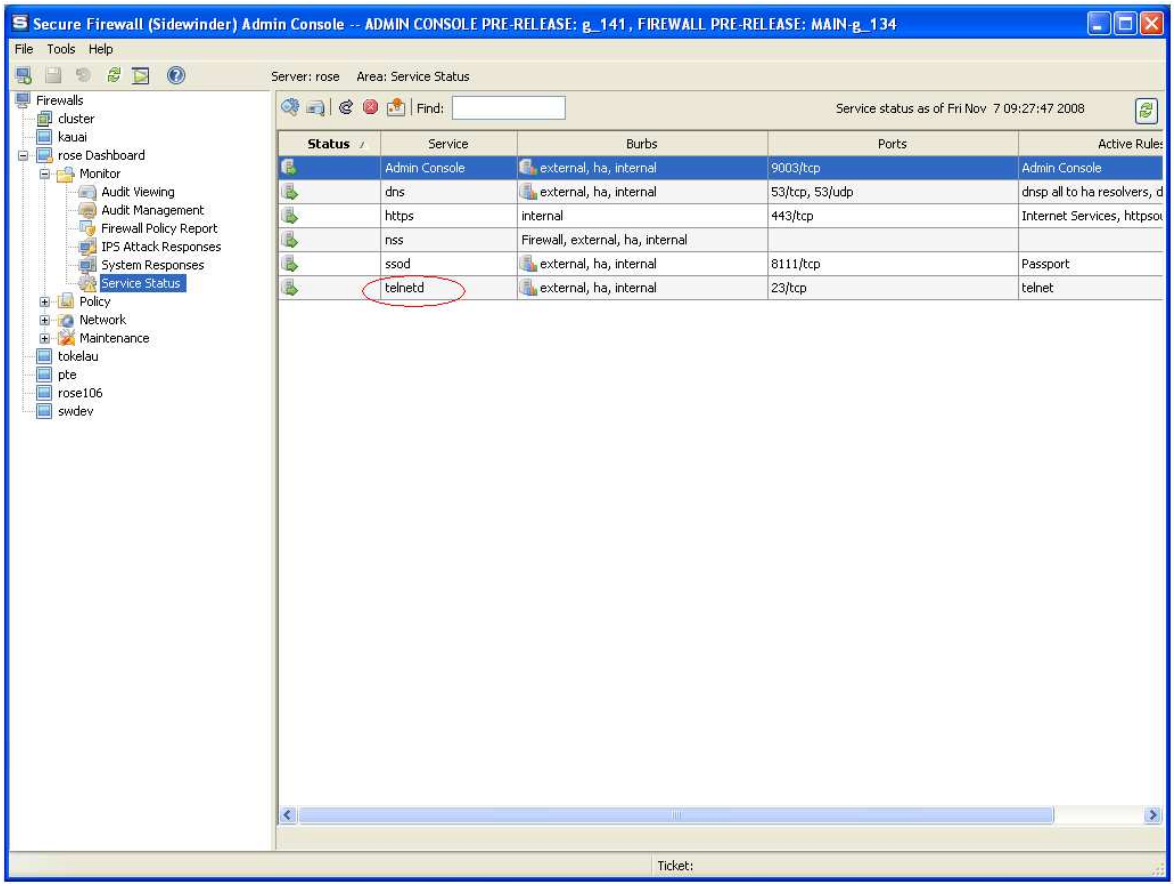


Figure 20 – Service Status

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 21).
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.

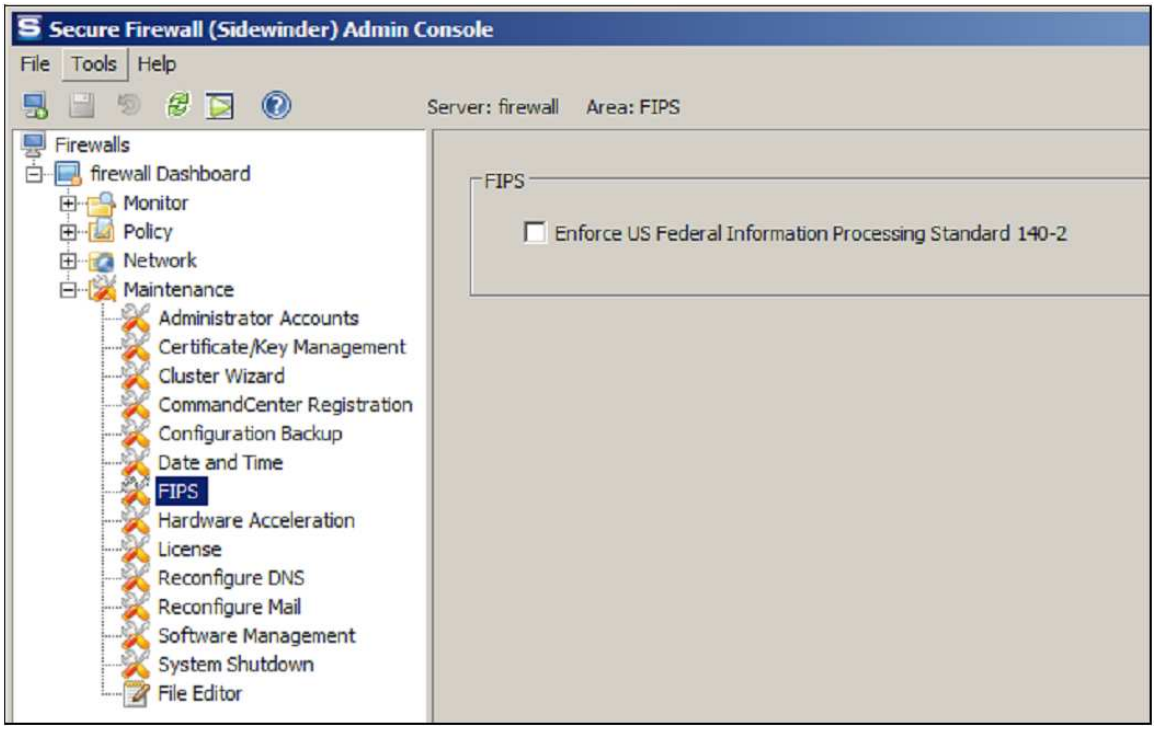


Figure 21 – Configuring For FIPS

Whether the module has been upgraded to **7.0.1.03** from an earlier firmware, or shipped with **7.0.1.03** 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 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 17.

Table 17 – 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[33] 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

[33] HTTPS – Hypertext Transfer Protocol Secure

Services	Cryptographic Keys/CSPs
Administrator Passwords	Firewall Certificate/private key

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

3.1.2 Management

The module can run in two different modes: FIPS-Approved and non-FIPS-Approved. While in a 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 FIPS mode of operation and active bypass mode. The CO also monitor that only FIPS-Approved algorithms as listed in Table 12 are being used for TLS and SSH sessions.

The "show status" for FIPS mode of operation can be invoked by determining if the checkbox, shown in Figure 21, is checked. 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.

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

3.1.3 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 17. 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.

3.1.4 Disabling FIPS Mode of Operation

To take the module out of FIPS mode of operation, the Crypto-Officer must zeroize the CSPs as described in section 3.1.3 of this document. FIPS mode can be disabled from Admin Console window:

1. Select "**Maintenance / FIPS**". The FIPS check box appears in the right pane.
2. Unselect "**Enforce U.S. Federal Information Processing Standard**" (shown in Figure 21).
3. Save the configuration change.
4. Select "**Maintenance / System Shutdown**" and reboot the firewall to the Operational kernel to activate the change.

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 18 – 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
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
DAC	Data Authentication Code
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

Acronym	Definition
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
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
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

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

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