McAfee, Inc.

McAfee Firewall Enterprise 2150E

Hardware Version: 2150E; Firmware Version: 7.0.1.01.E12

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.4

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.
10340 Democracy Lane, Suite 201
Fairfax, Virginia 22030
United States of America

Phone: +1 (703) 267-6050

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

Prepared by:
Email: info@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 2150E from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise 2150E meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The McAfee Firewall Enterprise 2150E is referred to in this document as the 2150E, the crypto-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 McAfee Firewall Enterprise 2150E

2.1 Overview

McAfee, Inc. is a global leader in Enterprise Security solutions. The company's comprehensive portfolio of network security products and solutions provides unmatched protection for the enterprise in the most mission-critical and sensitive environments. McAfee's McAfee Firewall Enterprise 2150E 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, the McAfee Firewall Enterprise 2150E appliance is the strongest self-defending perimeter firewall 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.

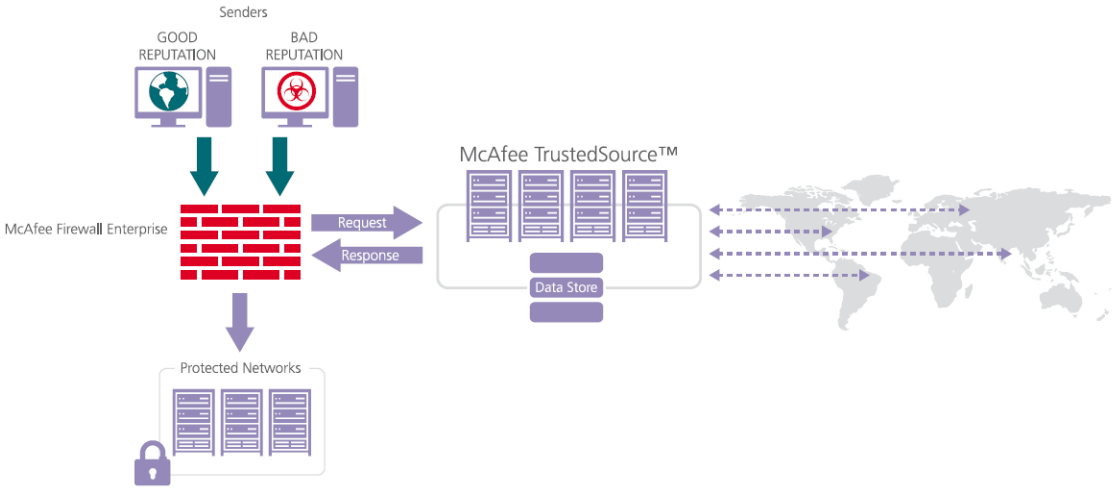

Figure 1 – Typical Deployment Scenario

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 CommandCenter 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) for remote Internet Protocol (IP) monitoring
- 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 McAfee McAfee Firewall Enterprise 2150E and that no CSPs or user data are transmitted over this interface.

McAfee Firewall Enterprise 2150E is a 2U rack-mountable appliance appropriate for mid- to large-sized organizations. A front view of the cryptographic module is shown in Figure 2 below.

Figure 2 – McAfee Firewall Enterprise 2150E

The McAfee Firewall Enterprise 2150E is validated at the following FIPS 140-2 Section levels:

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

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

Section	Section Title	Level
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 McAfee Firewall Enterprise 2150E is a multi-chip standalone hardware module that meets overall level 2 FIPS 140-2 requirements. The cryptographic boundary of the 2150E is defined by the hard metal chassis, which surrounds all the hardware and software components.

2.3 Module Interfaces

The McAfee Firewall Enterprise 2150E is a multi-chip standalone cryptographic module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the 2150E is defined by the metal chassis, which surrounds all the hardware and software components. 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

All ports and interfaces are located at the front or back side of the hardware module. The front bezel of the chassis exposes a power button and a Liquid Crystal Display (LCD). The rear side of the module is populated with the following ports and interfaces:

- Four (4) Ethernet ports
- Two (2) Gigabyte Ethernet ports
- Two (2) Universal Serial Bus (USB) ports
- One (1) serial port
- One (1) Video Graphics Array (VGA) port
- Several Light-Emitting Diodes (LEDs)
- Power button

The ports and interfaces on the module's connector panel are mapped to logical interfaces in Table 2 below. All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

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

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Interface	McAfee Firewall Enterprise 2150E Physical Ports
Data Input	Ethernet port
Data Output	Ethernet ports
Control Input	Ethernet ports, serial port, USB ports, power button
Status Output	Ethernet ports, serial port, USB ports, VGA port, LEDs
Power	Power connector

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 table indicate the type of access required using the following notation:

- Read: The CSP is read
- Write: The CSP is established, generated, modified, or zeroized
- 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 the protected 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, while remote access is via Secure Shell (SSH) session. The CO authenticates to the module using a username and password.

The crypto-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 3 below.

Table 3 – Crypto-Officer Services

Service	Description	Type of Access
Authenticate to the Admin Console	Used when administrators login to the appliance using the Firewall Enterprise Admin Console	Write, execute
Authenticate to the Admin Console using Command Access Card (CAC)	Used when administrators login to the appliance with CAC authentication to access the Firewall Enterprise Admin Console	Read, write, execute
Authenticate to the Admin CLI	Used when administrators login to the appliance using the Firewall Enterprise Admin CLI	Write, execute
Authenticate to the Admin CLI using CAC	Used when administrators login to the appliance with CAC authentication to access the Firewall Enterprise Admin CLI	Read, write, execute
Change password	Allows external users to use a browser to change their Firewall Enterprise, SafeWord PremierAccess, or LDAP login password	Write, execute
Configure cluster communication	Services required to communicate with each other in Firewall Enterprise multi-appliance configurations	Read, write, execute
Configure and monitor Virtual Private Network (VPN) accounts	Used to generate and exchange keys for VPN sessions and configure the user accounts	Read, write, execute
Create and configure bypass mode	Create and monitor IPsec policy table that governs alternating bypass mode	Read, write, execute
Manage mail services	Used when running 'sendmail' service on a Firewall Enterprise appliance	Read, write, execute
Manage web filter	Manages configuration with the SmartFilter	Read, write, execute

Service	Description	Type of Access
Manage CommandCenter communication	Verifies registration and oversees communication among the CommandCenter and managed Firewall Enterprise appliances	Read, write, execute
Monitor status on SNMP	Monitors non security relevant status of the module via SNMP v3	Read
Perform self-tests	Run self-tests on demand	Execute
Enable FIPS mode	Configures the module in FIPS mode	Read, write, execute
Show status	Allows Crypto-Officer to check whether FIPS mode is enabled	Write, execute
Zeroize	Zeroizes the module to the factory default state	Write, execute

2.4.2 User Role

The User role has the ability to utilize the module's data transmitting functionalities via Ethernet port. Descriptions of the services available to the Users are provided in the table below.

Table 4 – User Services

Service	Description	Type of Access
Encrypt/decrypt	Allow secure VPN into corporate network over IPsec tunnel	Execute
Bypass	Access bypass capabilities of the module	Execute

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. The CO defines security policy rules as to how a Network User is to communicate with other devices or computers. Table 5 lists all the services that are available to the Network User role.

Table 5 – Network User Services

Service	Description	Type of Access
Communicate within the network	Communicate with other devices or computers within the network	Read

2.4.4 Authentication Mechanism

The module employs the following authentication methods to authenticate Crypto-Officer, Users, and Network Users.

Table 6 – Authentication Mechanisms Employed by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Alphanumeric characters can be used with repetition, which gives a total of 62 characters to choose from. The chance of a random attempt falsely succeeding is $1:62^8$, or 1:218,340,105,584,896.
	Common Access Card	The Common Access Card has a maximum password length of 128 characters. However, one time passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. Alphanumeric characters can be used with repetition, which gives a total of 62 characters to choose from. The chance of a random attempt falsely succeeding is $1:62^8$, or 1:218,340,105,584,896.
User	Password	Passwords are required to be at least 6 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Alphanumeric characters can be used with repetition, which gives a total of 62 characters to choose from. The chance of a random attempt falsely succeeding is $1:62^6$, or 1: 56,800,235,584.
Network User	Password, Certificate, or IP Address	Passwords are required to be at least 6 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Alphanumeric characters can be used with repetition, which gives a total of 62 characters to choose from. The chance of a random attempt falsely succeeding is $1:62^6$, or 1:56,800,235,584. Certificates used as part of TLS, SSH, and IKE[6]/IPsec

[6] IKE – Internet Key Exchange

Role	Type of Authentication	Authentication Strength
		are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is $1:2^{80}$, or $1:120,893 \times 10^{24}$. The module also authenticates network users by IP address via firewall rules.

2.5 Physical Security

The McAfee Firewall Enterprise 2150E is a multi-chip standalone cryptographic module. The module is contained in 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. There are only a limited set of louvered vent holes provided in the cases, and these holes obscure the view of the internal components of the module. Tamper-evident labels are applied to the case to provide physical evidence of attempts to remove the case. The placement of tamper-evident labels can be found in Secure Operation section of this document. The tamper-evidence labels need to be inspected periodically for tamper evidence.

The 2150E system has been tested and found conformant to the Electromagnetic Interference/Electromagnetic Compatibility (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 McAfee Firewall Enterprise 2150E, because the module does not provide a general-purpose operating system (OS) to the user. The OS has limited operational environment and only the module's custom written image can be run on the system. 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 implements three firmware cryptographic libraries to offer secure networking protocols and cryptographic functionalities. The firmware libraries are the Cryptographic Library for SecureOS® (CLSOS) Version 7.0.1 for 32/64-bit systems and the Kernel Cryptographic Library for SecureOS® (KCLSOS) Version 7.0.1. Security functions offered by the libraries in FIPS mode of operation map to the certificates listed in Table 7.

Table 7 – Algorithm Certificate Numbers for Cryptographic Libraries

Approved or Allowed Security Functions	64-bit Cryptographic Library for SecureOS®	32-bit Cryptographic Library for SecureOS®	Kernel Cryptographic Library for SecureOS®
Symmetric Key Algorithm			

Approved or Allowed Security Functions	64-bit Cryptographic Library for SecureOS®	32-bit Cryptographic Library for SecureOS®	Kernel Cryptographic Library for SecureOS®
Advanced Encryption Standard (AES) 128-, 192-, 256-bit in CBC[7], and ECB[8] modes	972	973	974
AES 128-, 192-, 256-bit in CFB[9]128 mode (FIPS non-compliant)	N/A	N/A	N/A
Triple-DES[10] – 112- and 192-bit in CBC mode	765	766	767 (192-bit only)
Secure Hashing Algorithm (SHA)			
SHA-1, SHA-256, SHA-384, and SHA-512	941	942	943
Message Authentication Code (MAC) Function			
HMAC[11] using SHA-1, SHA-256, SHA-384, and SHA-512	544	545	546
Pseudo Random Number Generator (PRNG)			
ANSI[12] X9.31 Appendix A.2.4 PRNG with 256-bit AES	549	550	551
Asymmetric Key Algorithm			
RSA[13] PKCS[14] #1 sign/verify: 1024-, 2048-, 4096-bit	469	470	Not implemented
RSA ANSI X9.31 key generation: 1024-, 2048-, 4096-bit	469	470	Not implemented
Digital Signature Algorithm (DSA) sign/verify – 1024-bit	338	339	Not implemented
Diffie-Hellman (DH) key agreement: 1024 and 2048 bits[15]	N/A	N/A	Not implemented
RSA encrypt/decrypt[16] (key transport)	N/A	N/A	Not implemented

[7] CBC – Cipher-Block Chaining
[8] ECB – Electronic Codebook
[9] CFB – Cipher Feedback Block
[10] DES – Data Encryption Standard
[11] HMAC – (Keyed-)Hash MAC
[12] ANSI – American National Standards Institute
[13] RSA – Rivest, Shamir, and Adleman
[14] PKCS – Public Key Cryptography Standard
[15] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)
[16] Caveat: RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength)

The module also implements the following non-approved algorithms to be used in non-FIPS mode of operation.

Table 8 – Non-approved Security Functions Implemented in the Module

Approved or Allowed Security Functions	64-bit Cryptographic Library for SecureOS®	32-bit Cryptographic Library for SecureOS®	Kernel Cryptographic Library for SecureOS®
Blowfish	Implemented	Implemented	Not implemented
Rivest Cipher (RC) 4	Implemented	Implemented	Not implemented
RC2	Implemented	Implemented	Not implemented
Message Digest (MD) 5	Implemented	Implemented	Not implemented
Single DES	Implemented	Implemented	Not implemented

The module supports the CSPs listed below in Table 9.

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

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMP v3 Session Key	AES 128-bit CFB Key	Internally generated but not FIPS Compliant	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Provides secured channel for SNMP v3 management that is not FIPS-approved
Common Access Card Authentication keys	RSA 1024-, 2048-bit keys or DSA 1024-, 2048-bit keys	Imported electronically in plaintext	Never exits the module	Resides in plaintext on volatile memory	Power cycle or session termination	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 key	Internally generated or imported electronically in plaintext via local management port	Encrypted form over Network port or local management port in plaintext	Stored in plaintext on the hard disk	By command	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
Peer public keys	RSA 1024-, 2048-, 4096-bit keys, DSA 1024-bit keys	Imported electronically in plaintext during handshake protocol	Never exit the module	Resides in plaintext on volatile memory	Power cycle or session termination	Peer Authentication for SSH and IKE sessions

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Local CA[17] public/private keys	RSA 1024,2048,4096-bit keys, DSA 1024-bit keys	Internally generated	Public key certificate exported electronically in plaintext via local management port	Stored in plaintext on the hard disk	By command	Local signing of firewall certificates and establish trusted point in peer entity
Key Establishment keys	Diffie-Hellman 1024,2048-bit keys, RSA 1024,2048,4096-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

[17] CA – Certificate Authority

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
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	By command	Data encryption/decryption for IKE sessions
IPsec Session Authentication Key	HMAC SHA-1 key	- Imported in encrypted form over network port or local management port in plaintext - Internally generated - Manually entered	Never exits the module	- Stored in plaintext on the hard disk - Resides in volatile memory	By command or power cycle	Data authentication for IPsec sessions
IPsec Session Key	Triple-DES, AES-128, AES-256	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Data encryption/decryption for IPsec sessions

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

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Administrator Passwords	PIN	Manually or electronically imported	Never exits the module	Stored on the hard disk through one-way hash obscurement	By command	Standard Unix authentication for administrator login
Common Access Card one-time password	8 character 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
ANSI X9.31 PRNG seed	16 bytes of seed value	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS approved random number
ANSI X9.31 PRNG key	AES-128	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS approved random number

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

The 2150E performs the following self-tests at power-up:

- Firmware integrity check using SHA-1 Error Detection Code (EDC)
- Approved 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 2150E performs the following conditional self-tests:

- Continuous PRNG Test (CRNGT) all implementations of FIPS-Approved and non-FIPS-Approved random number generator
- 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 in any of the tests listed above leads the module to a soft error state and logs an error message.

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 2150E meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

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 2150E appliance
- Media and Documents
- Activation Certificate
- Setup Guide
- Port Identification Guide
- Management Tools CD[18]
- Secure Firewall Installation Media USB drive (for appliances without a CD-ROM [19]drive)
- Power cord
- Rack mount kit

The Crypto-Officer is responsible for the proper initial setup of the Admin Console Management Tool software and the 2150E. 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 10 provides a list of available Firewall Enterprise documents.

Table 10 – 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 FIPS 140-2 Level 2	Includes procedures for hardware modifications, software updates, and configuration changes that meet FIPS 140-2 security requirements.
Secure Firewall CommandCenter Setup Guide	Leads through the initial CommandCenter configuration.
Secure Firewall	Complete administration information on all CommandCenter

[18] CD – Compact Disc
[19] CD-ROM – Compact Disc – Read-Only Memory

Document	Description
CommandCenter Administration Guide	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 Secure Firewall FIPS 140-2 Level 2 documents. 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 three activities to ensure that the module is running in an approved FIPS mode of operation:

- Apply tamper-evident labels
- Set FIPS environment
- Set FIPS mode enforcement

3.1.1.1 Applying Tamper-Evident Labels

The CO must put tamper-evident labels on the module as described in the table below. Prior to affixing the labels, the front bezel must be attached and the module powered up. The front bezel protects the removable components (hard drives and bays) at the front side. Additionally, the 2150E has removable power supplies and top panel. The labels should be placed on the appliance as shown in the figures below (indicated by the red circles). Instructions to put the label to secure the hard drives and the top panel are provided below.

1. Place a tamper-evident label overlapping front bezel and metal cover at the top to secure the disk drives, as shown in Figure 3.

Figure 3 – Tamper-Evident Label Application Instruction at the Front

2. The cryptographic module's top panel can be slide back and be removed. A label needs to be placed across the right side center as shown in Figure 4. The label should be placed such that it is affixed to both the top cover and side of the chassis.

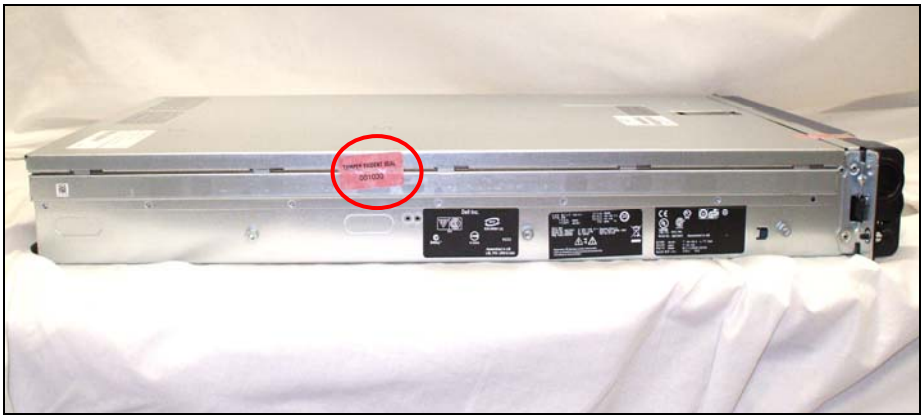

Figure 4 – Tamper-Evident Label Application Instruction at the Right Side

The removable power supplies at the rear side of the module, as shown in Figure 5, are excluded from the security requirement. Hence the power supplies do not require to be sealed with a tamper-evident label.

Figure 5 – Rear Panel of McAfee Firewall Enterprise 2150E

After the labels are placed as instructed above, the module can be powered up and the Crypto-Officer may proceed with initial configuration.

3.1.1.2 Setting FIPS Environment

The cryptographic module requires that firmware version 7.0.1.01 be upgraded with patch E12. While some models may have the patch version pre-installed, others may require upgrading. To check if the module is currently running version **7.0.1.01.E12**, the Crypto-Officer must open the GUI-based administrative 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.

To perform the upgrade, the Crypto-Officer must first check the firmware to ensure they are running version **7.0.1.01**. If this version is not running, the Crypto-Officer must take measures to upgrade the module to **7.0.1.01**. If required, this upgrade can be performed through the GUI-based administrative 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 update the module to **7.0.1.01.E12**, the Crypto-Officer must:

1. Under "**Software Management / Manage Packages**" table, select "70101.E12";
2. Select download;
3. Select install;
4. Verify that the "**Manage Packages**" tab states that "70101.E12" is installed.

3.1.1.3 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 6 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.

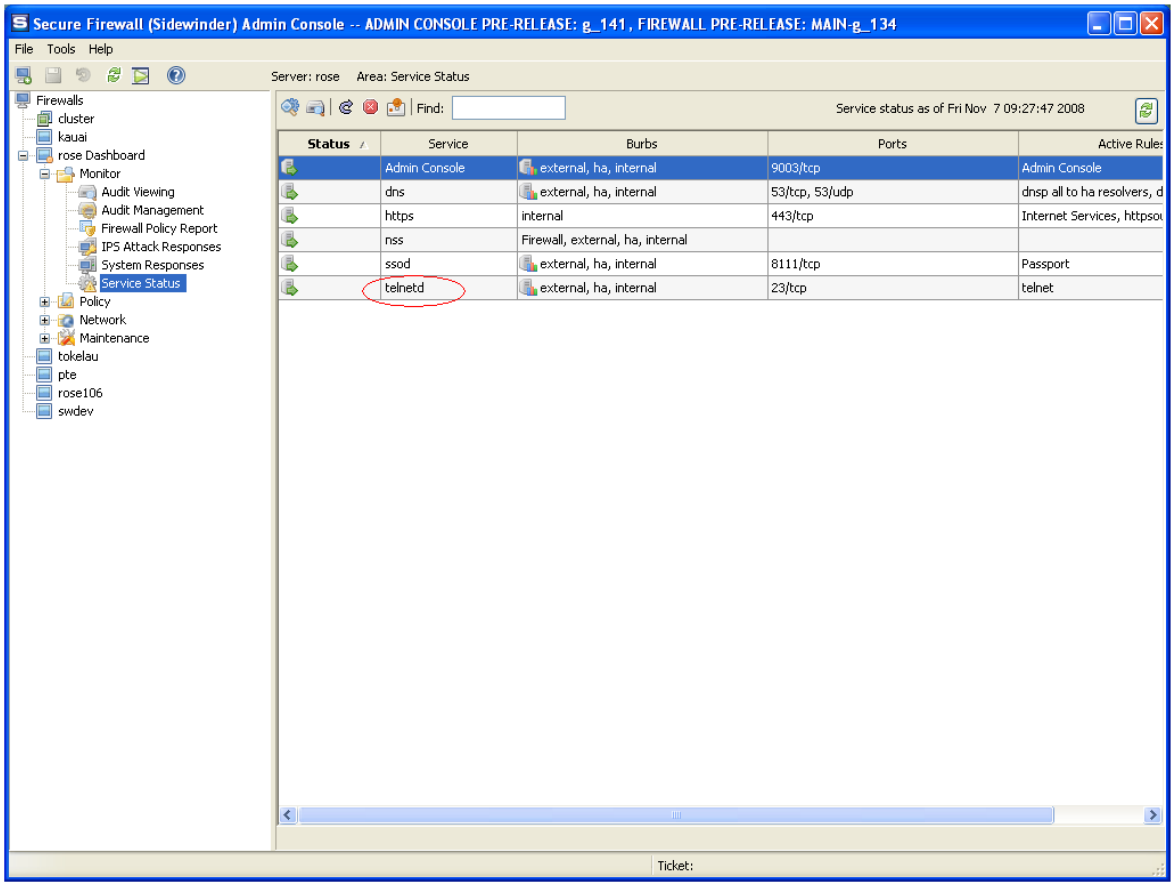

Figure 6 – Service Status

The process to enable FIPS mode is provided below:

1. Under **"Policy/Application Defences/ 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 7).
4. Select Enforce US 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.

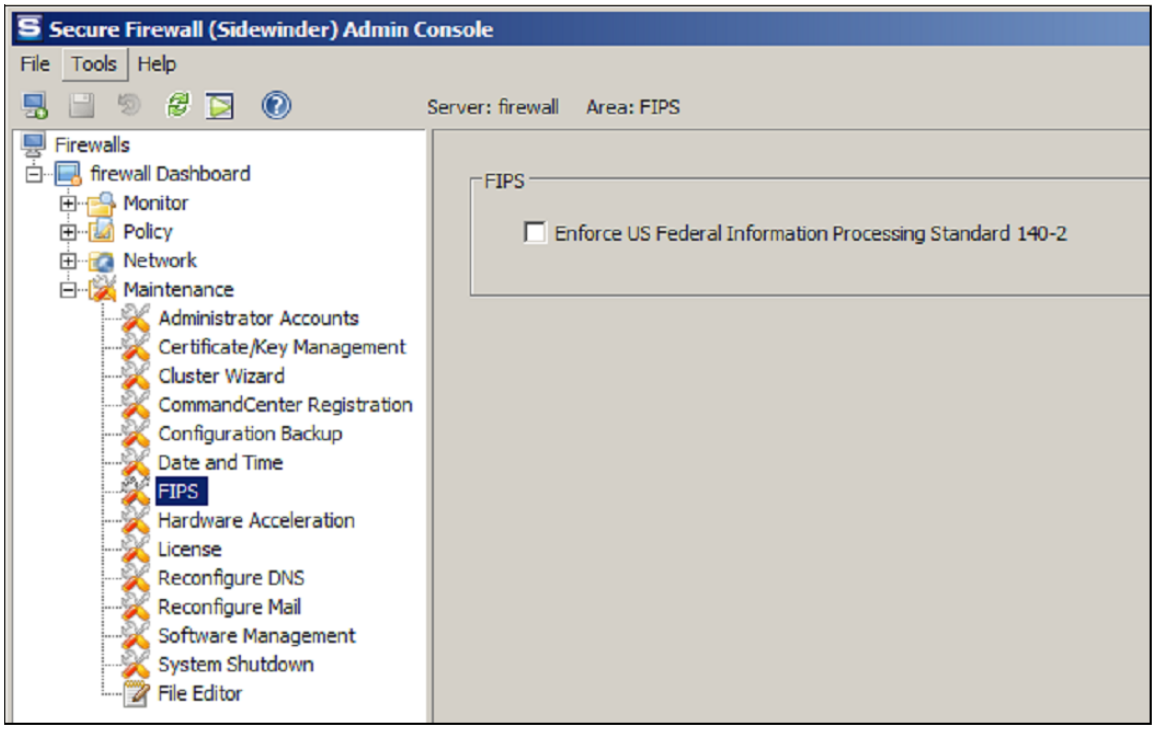

Figure 7 – Configuring For FIPS

Whether the module has been upgraded to **7.0.1.01** from an earlier firmware, or shipped with **7.0.1.01** 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 11.

Table 11 – Required Keys and CSPs for Secure Operation

Services	Cryptographic Keys/CSPs
Admin Console (TLS)	Firewall Certificate/private key
Command Center (TLS)	Firewall Certificate/private key
HTTPS[20] 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

[20] HTTPS – Hypertext Transfer Protocol Secure

Administrator Passwords	Firewall Certificate/private key

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

For troubleshooting or assistance with enabling FIPS mode, the CO may opt to download the FIPS 140-2 Setup guide at the following location: http://mysupport.mcafee.com.

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 VGA port. 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 7 are being used for TLS and SSH sessions.

The show status for FIPS mode of operation can be invoked by checking if the checkbox, shown in Figure 7, 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. Once a factory reset has been performed, there will be some default keys and CSPs which were setup as part of the renewal process. These keys must be recreated as per the instructions found in Table 11. 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 US Federal Information Processing Standard (shown in Figure 7).
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 12 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher-Block Chaining
CD	Compact Disc
CD-ROM	Compact Disc – Read-Only Memory
CFB	Cipher Feedback
CLI	Command Line Interface
CLSOS	Cryptographic Library for SecureOS
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash Message Authentication Code
HTTPS	Hyper Text
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange

Acronym	Definition
IP	Internet Protocol
IPsec	Internet Protocol Security
KAT	Known Answer Test
KCLSOS	Kernel Cryptographic Library for SecureOS
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
MD	Message Digest
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NMS	Network Management System
OS	Operating System
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RC	Rivest Cipher
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
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.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

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