McAfee, Inc.

McAfee Firewall Enterprise 1100E, 2150E, and 4150E

Hardware Part Numbers: NSA-1100-FWEX-E, NSA-2150-FWEX-E, and NSA-4150-FWEX-E
Firmware Version: 8.3.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.9

Prepared for:

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

Phone: +1 408 988 3832
http://www.mcafee.com

Prepared by:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the McAfee Firewall Enterprise 1100E, 2150E, and 4150E from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise 1100E, 2150E, and 4150E appliances (Hardware Part Numbers: NSA-1100-FWEX-E, NSA-2150-FWEX-E, and NSA-4150-FWEX-E; Firmware Version: 8.3.1) 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 module in its 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 1100E, 2150E, and 4150E appliances are referred to in this document collectively as the MFE E-Series, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The McAfee corporate website (http://www.mcafee.com) contains information on the full line of products from McAfee.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Validation Submission Summary document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to McAfee. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to McAfee and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact McAfee.

2 MFE E-Series Appliances

2.1 Overview

McAfee, Inc. is a global leader in Enterprise Security solutions. The company's comprehensive portfolio of network security products and solutions provides unmatched protection for the enterprise in the most mission-critical and sensitive environments. The McAfee Firewall Enterprise 1100E, 2150E, and 4150E appliance line was created to meet the specific needs of organizations of all types and enable those organizations to reduce costs and mitigate the evolving risks that threaten today's networks and applications.

Consolidating all major perimeter security functions into one system, the McAfee Firewall Enterprise appliances are the strongest self-defending perimeter firewalls in the world. Built with a comprehensive combination of high-speed application proxies, reputation-based threat intelligence, and signature-based security services, Firewall Enterprise defends networks and Internet-facing applications from all types of malicious threats, both known and unknown.

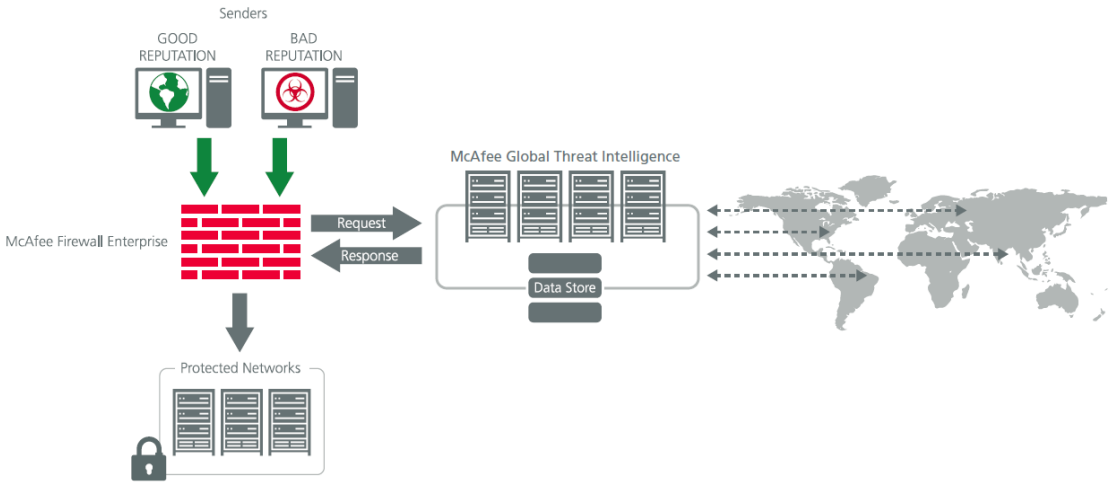


Figure 1 – Typical Deployment Scenario

Firewall Enterprise appliances are market-leading, next-generation firewalls that provide application visibility and control even beyond Unified Threat Management (UTM) for multi-layer security – and the highest network performance. Global visibility of dynamic threats is the centerpiece of Firewall Enterprise and one of the key reasons for its superior ability to detect unknown threats along with the known. Firewall Enterprise appliances deliver the best-of-breed in security systems to block attacks, including:

- Viruses
- Worms
- Trojans
- Intrusion attempts
- Spam and phishing tactics
- Cross-site scripting
- Structured Query Language (SQL) injections
- Denial of service (DoS)
- Attacks hiding in encrypted protocols

Firewall Enterprise security features include:

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

The MFE 1100E is a 1U rack-mountable appliance. The MFE 2150E is a 2U rack-mountable appliance. The MFE 4150E is an enterprise-class 5U rack-mountable appliance. All of these appliances are appropriate for mid- to large-sized organizations. The appliances are shown in Figure 2, Figure 3, and Figure 4 below.

Figure 2 – McAfee MFE 1100E

Figure 3 – McAfee MFE 2150E

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

Figure 4 – McAfee MFE 4150E

The MFE E-Series can be managed locally or remotely using one of the following management tools:

- Administration Console – The Administration Console (or Admin Console) is the graphical software that runs on a Windows computer within a connected network. Admin Console is McAfee's proprietary GUI management software tool, and needs to be installed on a Windows-based workstation. This is the primary management tool. All Admin Console sessions are protected over secure TLS channel.

- Command Line Interface (CLI) – A UNIX-based CLI is also available for configuring the firewall and performing troubleshooting functions. It can be used as an alternative to the Admin Console to perform most administration tasks. The CLI is accessed locally using a terminal or terminal emulator over the serial port or by a direct-connected keyboard and monitor. Remote access is via Secure Shell (SSH) session.

- MFE SNMP Agent – The MFE E-Series can use the SNMP v3 protocol for remote management, and to provide information about the state and statistics as part of a Network Management System (NMS).

  Although SNMP v3 can support AES encryption, the protocol employs a non-Approved key generation method. However, the module's SNMP Agent does not support "set" requests, preventing the modification of any critical security parameters (CSPs) through this interface. Additionally, because the module's CSPs are not defined in the Firewall's MIB[6], information about those CSPs is not made available to be transmitted or viewed over this interface. Thus, this interface provides management for non-FIPS-relevant information only, and offers no ability to alter or view CSPs.

- MFE Control Center – Control Center is an enterprise-class management appliance that enables scalable centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates, inventory their firewall products, generate reports, and demonstrate regulatory compliance. Control Center is designed to run on an administrator's workstation, and allows network administrators to fully mange their firewall solutions from the network edge to the core. Management communications between the MFE and Control Center are secured over a TLS session.

[6] MIB – Management Information Base

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

The MFE E-Series is validated at the FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level Per FIPS 140-2 Section

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

2.2 Module Specification

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

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

- McAfee Firewall Enterprise 32-bit Cryptographic Engine v8.3
- McAfee Firewall Enterprise 64-bit Cryptographic Engine v8.3
- Kernel Cryptographic Library for SecureOS® (KCLSOS) v8.2

Security functions offered by the libraries in the module's Approved mode of operation (and their associated algorithm implementation certificate numbers) are listed in Table 2.

Table 2 – Approved/Allowed Security Functions

Approved Security Function	32-Bit	64-Bit	KCLSOS
Symmetric Key			
Advanced Encryption Standard (AES) 128/192/256-bit in CBC[8], ECB[9], OFB[10], CFB128[11] modes	2303	2305	-
AES 128/192/256-bit in CBC, ECB modes	-	-	1833

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

Approved Security Function	32-Bit	64-Bit	KCLSOS
Triple Data Encryption Standard (DES) 2-key and 3-key options in CBC, ECB, OFB, CFB64 modes	1451	1453	-
Triple DES 2-key and 3-key options in CBC mode	-	-	1185
Asymmetric Key			
RSA[12] ANSI[13] X9.31 key generation: 2048/3072-bit	1187	1189	-
RSA PKCS #1 signature generation: 2048/3072-bit	1187	1189	-
RSA PKCS #1 signature verification: 1024/1536/2048/3072/4096-bit	1187	1189	-
Digital Signature Algorithm (DSA) signature verification: 1024-bit	722	724	-
Secure Hash Standard			
SHA[14]-1, SHA-256, SHA-384, and SHA-512	1988	1990	1612
Message Authentication			
HMAC[15] using SHA-1, SHA-256, SHA-384, and SHA-512	1418	1420	1086
Random Number Generation (RNG)			
ANSI X9.31 Appendix A.2.4 PRNG	1146	1148	964
Key Agreement Schemes (KAS)			
Diffie-Hellman (DH): 2048-bit[16]	Non-approved, but allowed	Non-approved, but allowed	-
Key Transport Schemes			
RSA encrypt/decrypt[17] 2048/3072-bit	Non-approved, but allowed	Non-approved, but allowed	-

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

- *Two-key Triple DES[18]*
- *1024-bit DSA digital signature verification*
- *1024/1536-bit RSA digital signature verification*

The module also includes the following non-compliant algorithms:

- 1024/1536/4096-bit RSA PKCS #1 signature generation
- 1024/1536/4096-bit RSA ANSI X9.31 key generation
- 1024-bit Diffie-Hellman
- 1024/1536/4096-bit RSA encrypt/decrypt

[12] RSA – Rivest, Shamir, and Adleman
[13] ANSI – American National Standards Institute
[14] SHA – Secure Hash Algorithm
[15] HMAC – (Keyed-) Hash Message Authentication Code
[16] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
[17] Caveat: RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
[18] Caveat: To use the two-key Triple DES algorithm to encrypt data (or wrap keys) in an Approved mode of operation, the module operator shall ensure that the same two-key Triple DES key is not used for encrypting data (or wrapping keys) with more than 2^{20} plaintext data (or plaintext keys).

Additionally, the module employs a hardware RNG which acts as an entropy-gathering mechanism to provide seeding material for KCLSOS PRNG.

2.3 Module Interfaces

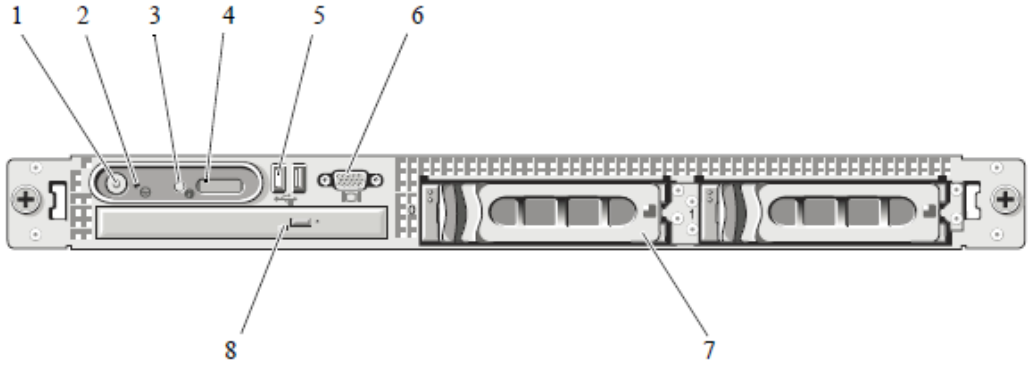
Interfaces on the module can be categorized as the following FIPS 140-2 logical interfaces:

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

The physical ports and interfaces for the various models are shown below. Note the following acronyms used in the figures below:

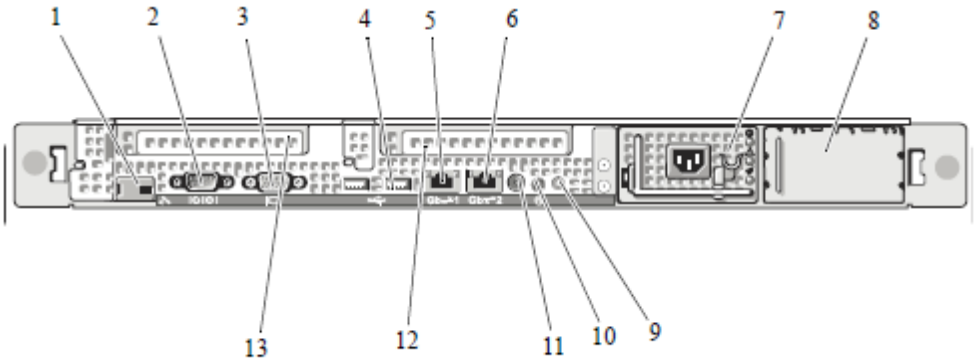
- LCD – Liquid Crystal Display
- NIC – Network Interface Card
- NMI – Non-Maskable Interrupt
- PCI - Peripheral Component Interconnect
- USB – Universal Serial Bus

The physical ports and interfaces for the MFE 1100E are depicted in Figure 5 and Figure 6 below.



1	Power-on indicator, power button	5	USB connectors (2)
2	NMI button	6	Video connector
3	System identification button	7	Hard drives (optional)
4	LCD display	8	Optical drive (optional)

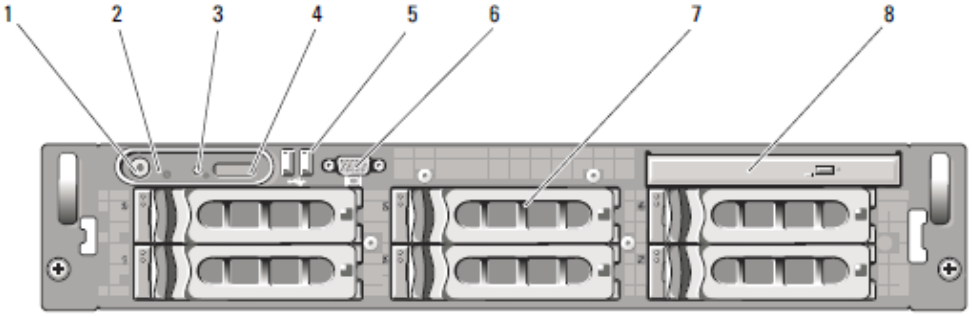
Figure 5 – 1100E Front Panel Features and Indicators



1	remote access controller (optional)	2	serial connector	3	video connector
4	USB connectors (2)	5	NIC1 connector	6	NIC2 connector
7	power supply 1	8	power supply 2 (optional)	9	system status indicator
10	system identification button	11	system status indicator connector	12	left PCI expansion slot (slot 2)
13	center PCI expansion slot (slot 1)				

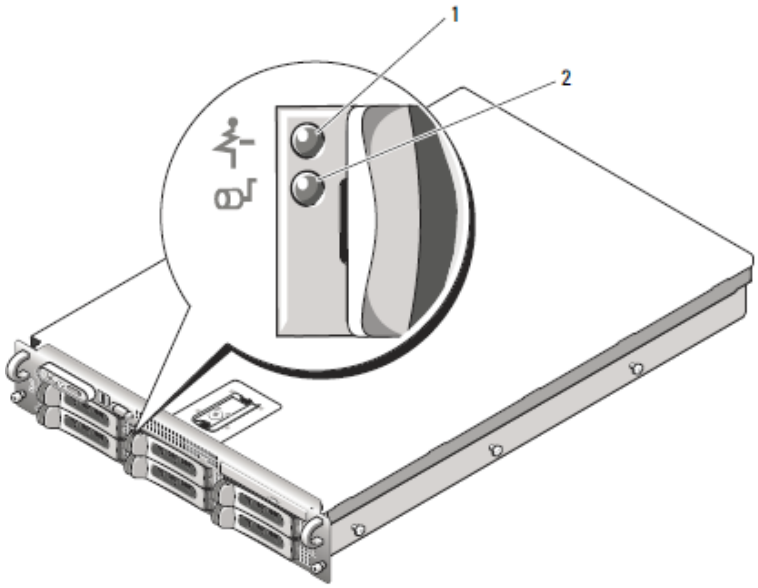
Figure 6 – 1100E Back Panel Features and Indicators

The physical ports and interfaces for the MFE 2150E are depicted in Figure 7, Figure 8, and Figure 9 below



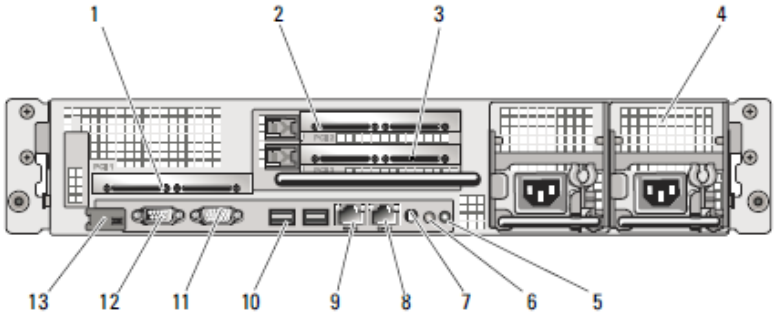
1	Power-on indicator, power button	5	USB connectors (2)
2	NMI button	6	Video connector
3	System identification button	7	Hard drives (8)
4	LCD panel	8	Optical drive (optional)

Figure 7 – 2150E Front Panel Features and Indicators



1	drive-status indicator (green and amber)	2	green drive-activity indicator

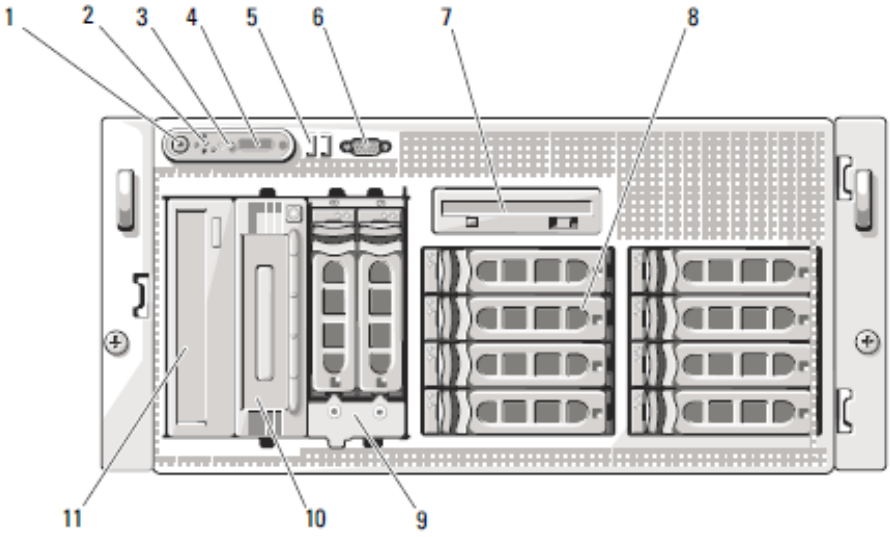
Figure 8 – 2150E Hard Drive Indicators



1	center PCI riser (slot 1)	2	left PCI riser (slot 2)	3	left PCI riser (slot 3)
4	power supplies (2)	5	system identification button	6	system status indicator
7	system status indicator connector	8	NIC2 connector	9	NIC1 connector
10	USB connectors (2)	11	video connector	12	serial connector
13	remote access controller (optional)				

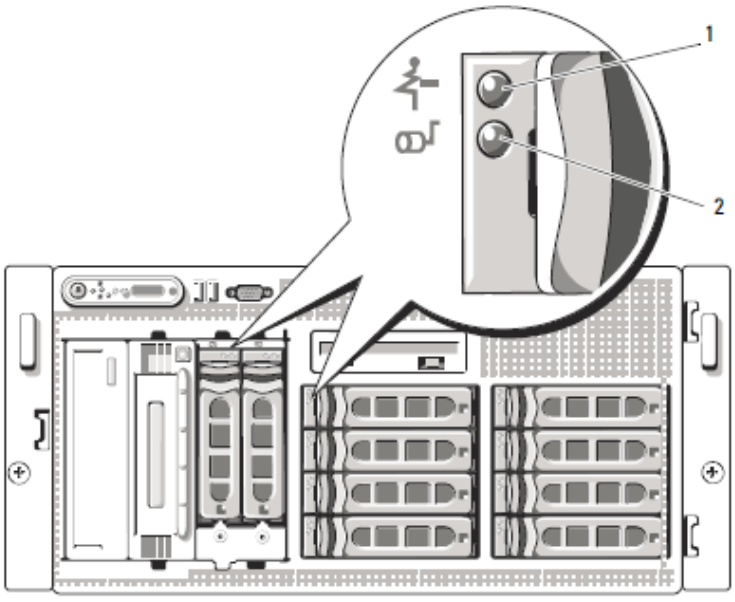
Figure 9 – 2150E Back Panel Features and Indicators

The physical ports and interfaces for the MFE 4150E are depicted in Figure 10, Figure 11, and Figure 12 below.



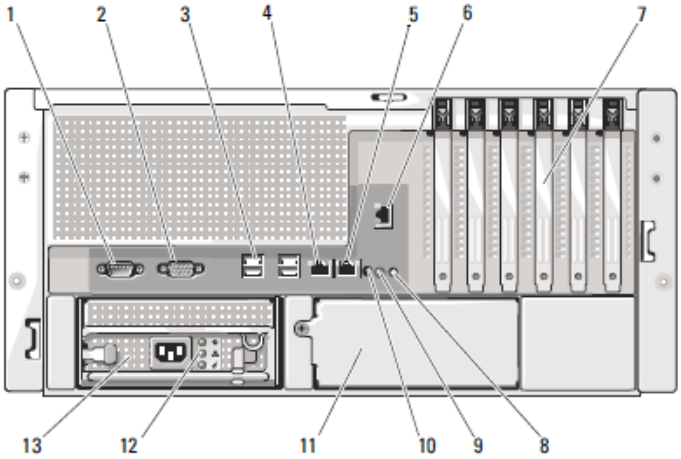
1	Power-on indicator, power button	6	Video connector
2	NMI button	7	Diskette drive
3	System identification button	8	Hard drives
4	LCD panel	9	Flex bay
5	USB connectors (2)	10	Tape backup unit
		11	Optical drive

Figure 10 – 4150E Front Panel Features and Indicators



1	drive-status indicator (green and amber)	2	green drive-activity indicator

Figure 11 – 4150E Hard Drive Indicators



1	serial connector	2	video connector	3	USB connectors (4)
4	NIC1 connector	5	NIC2 connector	6	remote access connector (optional)
7	expansion-card slots (6)	8	system status indicator	9	system identification button
10	system status indicator connector	11	power supply 2 (optional)	12	power supply status indicators
13	power supply 1				

Figure 12 – 4150E Back Panel Features and Indicators

All of these physical interfaces map to logical interfaces (as defined by FIPS 140-2) as described in Table 3.

Table 3 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Module Interface
Data Input	Connectors (network)
Data Output	Connectors (network)
Control Input	Buttons (NMI, power, LCD panel, system identification) and connectors (network, USB, serial)
Status Output	Connectors (video, network, serial), and LED indicators (power-on, drive activity, drive status, system status)
Power	Connectors (power)

A lockable metal bezel is mounted to each front of each appliance (see Figure 2, Figure 3, and Figure 4). The lock is used to prevent unauthorized access to system peripherals, hard drives, and the control panel. Of the available front panel features and indicators (see Figure 5, Figure 7, and Figure 10), only the LCD panel and hard drive LEDs are accessible when the bezel is installed.

2.4 Roles, Services, and Authentication

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

2.4.1 Authorized Roles

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

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

- User – Users employ the services of the module for establishing VPN[19] connections or TLS connections thru an IPsec tunnel via Ethernet port.

2.4.2 Services

The services that require operators to assume an authorized role (Crypto-Officer or User) are listed in Table 4 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 4 use the following indicators to show the type of access required:

- **R (Read)**: The CSP is read
- **W (Write)**: The CSP is established, generated, modified, or zeroized
- **X (Execute)**: The CSP is used within an Approved or Allowed security function or authentication mechanism

Table 4 – Authorized Operator Services

Service	Description	Role		CSP and Type of Access
		CO	User	
Authenticate to the Admin Console	Allows administrators to login to the appliance using the Firewall Enterprise Admin Console	x		Administrator Password - R
Authenticate to the Admin Console using Common Access Card (CAC)	Allows administrators to login to the appliance with CAC authentication to access the Firewall Enterprise Admin Console	x		Common Access Card Authentication key - R
Authenticate to the Admin CLI	Allows administrators to login to the appliance using the Firewall Enterprise Admin CLI	x		Administrator Password - R
Authenticate to the Admin CLI using CAC	Allows administrators to login to the appliance with CAC authentication to access the Firewall Enterprise Admin CLI	x		Common Access Card Authentication key - R

[19] VPN – Virtual Private Network

Service	Description	Role		CSP and Type of Access
		CO	User	
Authenticate to the local console	Allows administrators to login to the appliance via the local console	x		Administrator Password - R
Change password	Allows external users to use a browser to change their Firewall Enterprise, SafeWord PremierAccess, or LDAP login password	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrator Password - R/W
Manage network objects	Allows administrators to view, create, and maintain network objects, manage netgroup memberships, and manage access control rules' time periods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure identity validation method	Allows administrators to select identity validation settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure cluster communication	Provides services required to communicate with each other in Firewall Enterprise multi-appliance configurations	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure and monitor Virtual Private Network (VPN) services	Generates and exchanges keys for VPN sessions	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W IKE Preshared key - W IPsec Session Key - W IPsec Authentication Key - W
Create and configure bypass mode	Creates and monitors IPsec policy table that governs alternating bypass mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage web filter	Manages configuration with the SmartFilter	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage Control Center communication	Verifies registration and oversees communication among the Control Center and managed Firewall Enterprise appliances	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	Role		CSP and Type of Access
		CO	User	
Configure Network Integrity Agent (NIA) settings	Configures NIA authentication and certificate settings, enable agent discovery, modify connection settings, and create explicit NIA communication rules	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure content inspection settings	Configures settings for content inspection methods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage applications and Application Defense information	Manages applications, application groups, and Application Defense settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage access control rules	Manages rules enforcing policy on network flows to or through the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage SSL rules	Manages SSL rules for processing SSL connections	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Process audit data	Allows administrators to view and export audit data, transfer audit records, and manage log files.	x		Firewall Authentication Keys - R Key Agreement Key - R DTLS Session Authentication Key - R/W DTLS Session Key - R/W
Manage attack and system responses	Configures how the firewall should respond to audit events that indicate abnormal and potentially threatening activities	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure network defenses	Customizes audit output for attacks on specific networks stopped by the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
View active hosts	Provides a method to view active hosts connected to a Firewall Enterprise appliance	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure the SNMP Agent	Configures the SNMP Agent for status monitoring of non-FIPS-relevant information	x		SNMP v3 Session Key - R

Service	Description	Role		CSP and Type of Access
		CO	User	
Configure networking	Configures and manages network characteristics, security zones, and Quality of Service profiles.	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage email services	Manages email options and 'sendmail' features	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Perform self-tests	Run self-tests on demand via reboot	x		None
Enable FIPS mode	Configures the module in FIPS mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Show status	Allows Crypto-Officer to check whether FIPS mode is enabled	x		None
Zeroize	Resets the module to its factory default state	x		Common Access Card Authentication keys - R/W Firewall Authentication public/private keys - R/W Peer public keys - R/W Local CA public/private keys - R/W IKE Preshared Key - R/W IPsec Session Authentication Key - R/W Administrator Password - R/W SSL CA key - R/W SSL Server Certificate key - R/W
Establish an authenticated TLS connection	Establish a TLS connection (requires operator authentication)		x	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W SSL CA key - R SSL Server Certificate key - R
Establish a VPN connection	Establish a VPN connection over IPsec tunnel		x	Firewall Authentication Keys - R Key Agreement Key - R IKE Session Authentication Key - W IKE Session Key - W IKE Preshared Key - R IPsec Session Key - R/W IPsec Authentication Key - R/W

2.4.3 Authentication Mechanisms

The module supports role-based authentication. Module operators must authenticate to the module before being allowed access to services which require the assumption of an authorized role. The module employs the authentication methods described in Table 5 to authenticate Crypto-Officers and Users.

Table 5 – 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 or Certificate	Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is $1:94^8$, or 1: 6,095,689,385,410,816. This would require about 60,956,893,854 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding. Certificates used as part of TLS, SSH, and IKE[20]/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is $1:2^{80}$, or 1: 1.20893×10^{24}. The fastest network connection supported by the module is 1000 Mbps. Hence, at most 60,000,000,000 bits of data ($1000 \times 10^6 \times 60$ seconds, or 6×10^{10}) can be transmitted in one minute. The passwords are sent to the module via security protocols IPsec, TLS, and SSH. These protocols provide strong encryption (AES 128-bit key at minimum, providing 128 bits of security) and require large computational and transmission capability. The probability that a random attempt will succeed or a false acceptance will occur is less than $1:2^{128} \times 94^4$.

2.5 Physical Security

The MFE E-Series is a multi-chip standalone cryptographic module. The module is contained in a hard metal chassis which is defined as the cryptographic boundary of the module. The module's chassis is opaque within the visible spectrum. The enclosure of the module has been designed to satisfy Level 2 physical security requirements. There are a limited number of louvered ventilation holes provided in the case, and these holes obscure the internal components of the module. 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 for each appliance can be found in Secure Operation section of this document.

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

[20] IKE – Internet Key Exchange

2.6 Operational Environment

The requirements in this section are not applicable, as the module does not provide a general-purpose operating system (OS) to module operators. McAfee's proprietary SecureOS version 8.3 provides a limited operational environment, and only the module's custom-written image can be run on the OS. The module provides a method to update the firmware in the module with a new version. This method involves downloading a digitally-signed firmware update to the module.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6. Note that the module generates cryptographic keys whose strengths are modified by available entropy. The available entropy is in the range of 114-128 bits.

.

Table 6 – 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 key	RSA 2048-bit key DSA 2048-bit key	Imported electronically in plaintext	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Common Access Card Authentication for generation of one-time password
Firewall Authentication public key	RSA 2048-bit key	Internally generated	Output in encrypted form via network port or in plaintext form via local management port	Stored in plaintext on the hard disk	Erasing the system image	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
	RSA 2048-bit key	Imported electronically in plaintext via local management port	Never exits the module	Resides in volatile memory in plaintext	Erasing the system image	
Firewall Authentication private key	RSA 2048-bit key	Internally generated	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
Peer public key	RSA 2048-bit key	Imported electronically in plaintext during handshake protocol	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Peer Authentication for TLS, SSH, and IKE sessions
Local CA[21] public key	RSA 2048-bit key	Internally generated	Public key certificate exported electronically in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Local signing of firewall certificates and establish trusted point in peer entity

[21] CA – Certificate Authority

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Local CA private key	RSA 2048-bit key	Internally generated	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Local signing of firewall certificates and establish trusted point in peer entity
Key Agreement Key	Diffie-Hellman 2048-bit key RSA 2048/3072-bit key	Internally generated	Public exponent electronically in plaintext, private component not exported	Resides in volatile memory in plaintext	Power cycle or session termination	Key exchange/agreement for DTLS, TLS, IKE/IPsec and SSH sessions
TLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for TLS sessions
TLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for TLS sessions
DTLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for DTLS sessions
DTLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for DTLS sessions
IKE Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for IKE sessions
IKE Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for IKE sessions
IKE Preshared Key	Triple-DES, AES-128, AES-256 key	- Imported in encrypted form over network port or local management port in plaintext - Manually entered	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Data encryption/decryption for IKE sessions

.

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

.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Common Access Card One-Time Password	8-character (minimum) ASCII string	Internally generated; Manually or electronically imported	Exported electronically in encrypted form over TLS	Resides in volatile memory inside the CAC Warder process	Password expiration, session termination, or power cycle	Common Access Card authentication for administrator login
MFE CE32 ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE32 ANSI X9.31 PRNG Key	AES-256 key	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE64 ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE64 ANSI X9.31 PRNG Key	AES-256 key	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
KCLSOS ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated from entropy sources	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
KCLSOS ANSI X9.31 PRNG Key	AES-256 key	Internally generated from entropy sources	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
SSL CA Key	RSA 2048-bit key DSA 2048-bit key	Internally generated	Exported electronically in ciphertext via network port or in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Signing temporary server certificates for TLS re-encryption
SSL Server Certificate Key	RSA 2048-bit key DSA 2048-bit key	Internally generated or imported electronically in plaintext via local management port	Exported electronically in ciphertext via network port or in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Peer authentication for TLS sessions (TLS re-encryption)

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

At power-up, the MFE E-Series automatically performs a firmware integrity check using HMAC SHA-256. The module also conducts cryptographic algorithm tests at power-up in the form of Known Answer Tests (KAT) and Pairwise Consistency Tests as list in Table 7 (note that the table indicates the library with which each test is associated).

Table 7 – Power-Up Cryptographic Algorithm Self-Tests

Algorithm Self-Test	32/64-Bit	KCLSOS
AES KAT for encrypt/decrypt	✓	✓
Triple-DES KAT for encrypt/decrypt	✓	✓
RSA KAT for sign/verify	✓	-
RSA KAT for encrypt/decrypt	✓	-
DSA pairwise consistency check	✓	-
SHA-1 KAT, SHA-256 KAT, SHA-384 KAT, and SHA-512 KAT	✓	✓
HMAC KAT with SHA-1, SHA-256, SHA-384, and SHA-512	✓	✓
ANSI X9.31 Appendix A.2.4 PRNG KAT	✓	✓

If any of the tests listed above fails to perform successfully, the module enters into a critical error state during which all cryptographic operations and output of any data is inhibited. An error message is logged for the CO to review and requires action on the Crypto-Officer's part to clear the error state.

2.8.2 Conditional Self-Tests

The McAfee Firewall Enterprise 1100E, 2150E, and 4150E conducts conditional cryptographic algorithm self-tests as indicated in Table 8 (again, note that the table indicates the library with which each test is associated).

Table 8 – Power-Up Cryptographic Algorithm Self-Tests

Algorithm Self-Test	32/64-Bit	KCLSOS
Continuous RNG Test (CRNGT)	✓	✓
RSA pairwise consistency test	✓	-
DSA pairwise consistency test	✓	-

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

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

Failure of the Bypass test or the KCLSOS PRNG CRNGT leads the module to a critical error state. Failure of any other conditional test listed above leads the module to a soft error state and logs an error message.

Upon reaching the critical error or soft error state, all cryptographic operations and data output is inhibited.

2.8.3 Critical Functions Self-Test

The MFE E-Series performs the following critical functions self-test at power-up:

- License Verification check

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

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

3.1 Crypto-Officer Guidance

The Crypto-Officer 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:

- MFE E-Series appliance
- Media and Documents
- Activation Certificate
- Setup Guide
- Port Identification Guide
- Management Tools CD[22]
- Firewall Enterprise Installation Media USB drive (for appliances without a CD-ROM[23] drive)
- Power cord
- Rack mount kit

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

The Crypto-Officer is responsible for the proper initial setup of the Admin Console Management Tool software and the cryptographic module. Setup of the Admin Console software is done by installing the software on an appropriate Windows® workstation (refer to the *McAfee Firewall Enterprise version 8.3.1 Product Guide* for details regarding installation of management tools) on the same network as the module. When you install the Admin Console, a link to the documents page is added to the "Start" menu of the computer. To view the Firewall Enterprise documents on the McAfee web site, select

Start > Programs > McAfee > Firewall Enterprise > Online Manuals

Table 9 provides a list of available Firewall Enterprise documents.

Table 9 – Summary of Firewall Enterprise Documentation

Document	Description
McAfee Firewall Enterprise version 8.3.x Quick Start Guide	Provides high-level instructions for setting up the firewall.
McAfee Firewall Enterprise version 8.3.1 Product Guide	Complete administration information on all firewall functions and features.
McAfee Firewall Enterprise version 8.3.1 Release Notes	Provides information about new features and enhancements introduced in version 8.3.1.

[22] CD – Compact Disc
[23] CD-ROM – Compact Disc – Read-Only Memory

.

Document	Description
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 the Firewall Enterprise Management Tools software. • 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 Firewall Enterprise 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. Initialization and configuration instructions for the module can also be found in the *McAfee Firewall Enterprise version 8.3.x Quick Start Guide*, *McAfee Firewall Enterprise version 8.3.1 Product Guide*, and this FIPS 140-2 Security Policy. The initial Administration account, including username and password for authenticating to the module, is created during the startup configuration process using the Quick Start Wizard.

The Crypto-Officer must perform these activities to ensure that the module is running in its Approved mode of operation:

1. Apply tamper-evident seals
2. Modify the BIOS[24]
3. Confirm the firmware version
4. 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. After the seals are placed as instructed below, the module can be powered up and the Crypto-Officer may proceed with initial configuration.

3.1.1.1.1 Prepare Module for Tamper-Evident Seal Application

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

3.1.1.1.2 1100E Tamper-Evident Seal Application

The 1100E has a removable front bezel and top panel that must be secured. Place two (2) tamper-evident seals on the appliance as indicated in red in Figure 13.

[24] BIOS – Basic Input/Output System

.

Figure 13 – 1100E Tamper-Evident Seal Application Positions (Seals #1 and 2)

The removable power supplies at the rear side of the module are excluded from the security requirements. Hence, the power supplies are not required to be sealed with a tamper-evident seal.

3.1.1.1.3 2150E Tamper-Evident Seal Application

The 2150E has a removable front bezel and top panel that must be secured. Place two (2) tamper-evident seals on the appliance as indicated in red in Figure 14 and Figure 15.

Figure 14 – 2150E Tamper-Evident Seal Application Position (Seal #1)

.

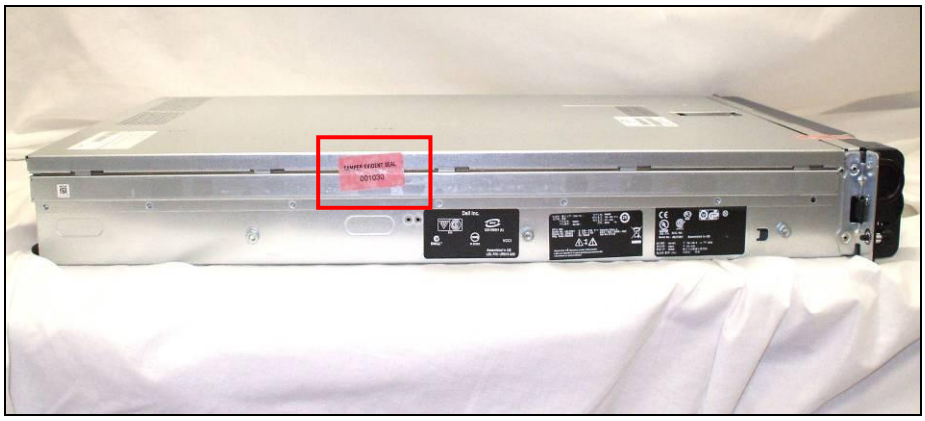


Figure 15 – 2150E Tamper-Evident Seal Application Position (Seal #2)

The removable power supplies at the rear side of the module are excluded from the security requirements. Hence, the power supplies are not required to be sealed with a tamper-evident seal.

3.1.1.1.4 4150E Tamper-Evident Seal Application

The 4150E has a removable front bezel and top panel that must be secured. Place four (4) tamper-evident seals on the appliance as indicated in red in Figure 16, Figure 17, and Figure 18.

Figure 16 – 4150E Tamper-Evident Seal Application Position (Seal #1)

.

Figure 17 – 4150E Tamper-Evident Seal Application Position (Seal #2)

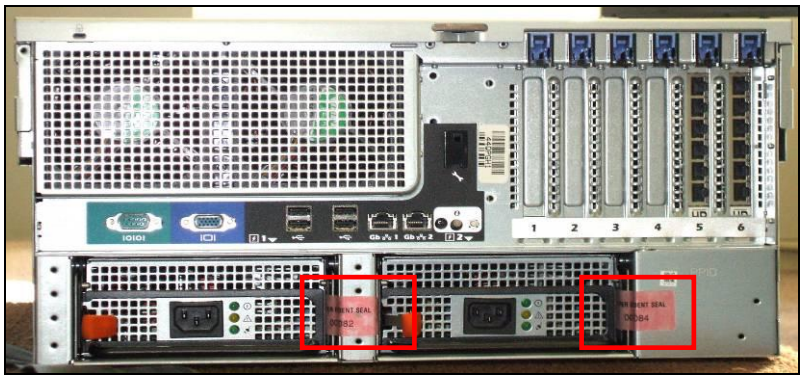


Figure 18 – 4150E Tamper-Evident Seal Application Positions (Seals #3 and #4)

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 operators 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):

1. From the command line, restart the firewall.
2. When the *F2 = System Setup* menu line appears in the upper right corner of the screen, press the <F2> key. The BIOS window appears.
3. To disable other bootable devices:
   a. Select **Boot Settings** and then press <Enter>.
   b. Select **Boot Sequence** and then press <Enter>.
   c. Verify that the hard drive is enabled. If necessary, use the space bar to enable the hard drive.
   d. Select all other devices and use the space bar to disable them.
   e. Press <Esc> to return to the main BIOS menu. Note: PXE[25] booting on Ethernet devices is not allowed. If PXE booting is enabled on an onboard NIC[26], select **Integrated Devices**,

[25] PXE – Preboot Execution Environment
[26] NIC – Network Interface Card

select the appropriate NIC, and use the right arrow to select **Enabled** (do not select **Enabled with PXE**).

4. To create a password for accessing the System Setup program and set the power recovery option:
   a. Select **System Security** and then press <Enter>.
   b. Select **Setup Password** and then press <Enter>.
   c. Enter a password and a confirmation and then press <Enter>.
   d. Select **AC Power Recovery** and then press <Right Arrow>.
   e. Use the space bar to set AC Power Recovery to "On".
   f. Press <Esc> twice to return to the main BIOS menu.
5. Press <Esc>, select **Save Changes and Exit**, and then press <Enter>. 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 / 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.

To perform the upgrade to version **8.3.1**, the Crypto-Officer must first check the firmware to ensure they are running version **8.2.1**. If this version is not running, the Crypto-Officer must first take measures to upgrade the module to **8.2.1**. 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 **8.2.1** to **8.3.1**, the Crypto-Officer must:

1. Under "**Software Management / Manage Packages**" table, select "8.3.1".
2. Select download.
3. Select install.
4. Verify that the "**Manage Packages**" tab states that "8.3.1" is installed.

3.1.1.4 Setting FIPS Mode Enforcement

Before enforcing FIPS on the module, the CO must check that no non-Approved service is running on the module.

Services and proxies are automatically enabled when rules are created that reference those services/proxies. To view the services that are currently used in enabled rules, select "**Policy / Access Control Rules**". The Access Control Rules window appears as shown in Figure 19 below. From here, select the "**Active Rules**" button in the upper right corner of the window (see Figure 20). If the Active Rules popup lists any non-Approved protocols, then those protocols must be disabled before the module is considered to be in its Approved mode of operation.

.

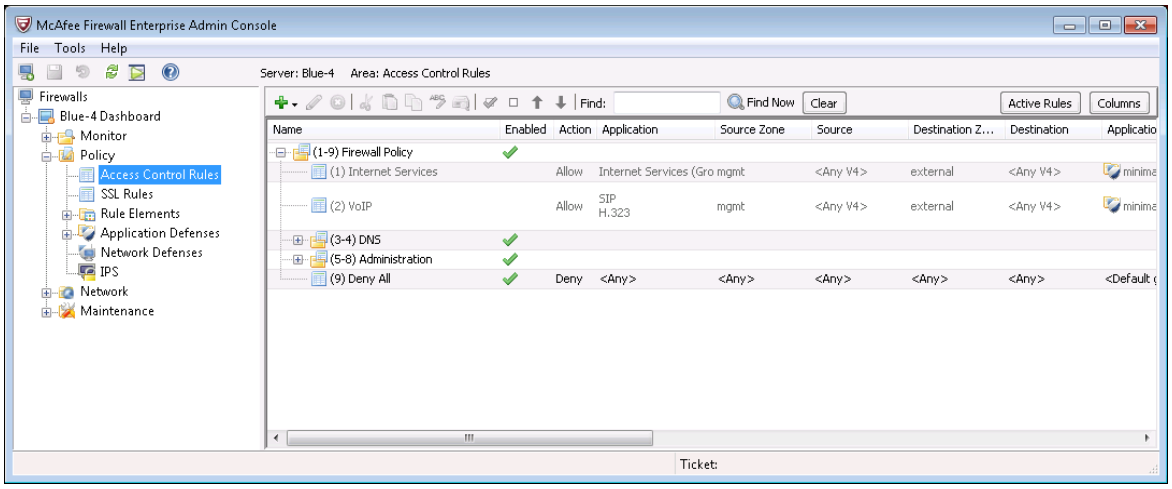


Figure 19 – Rules Window

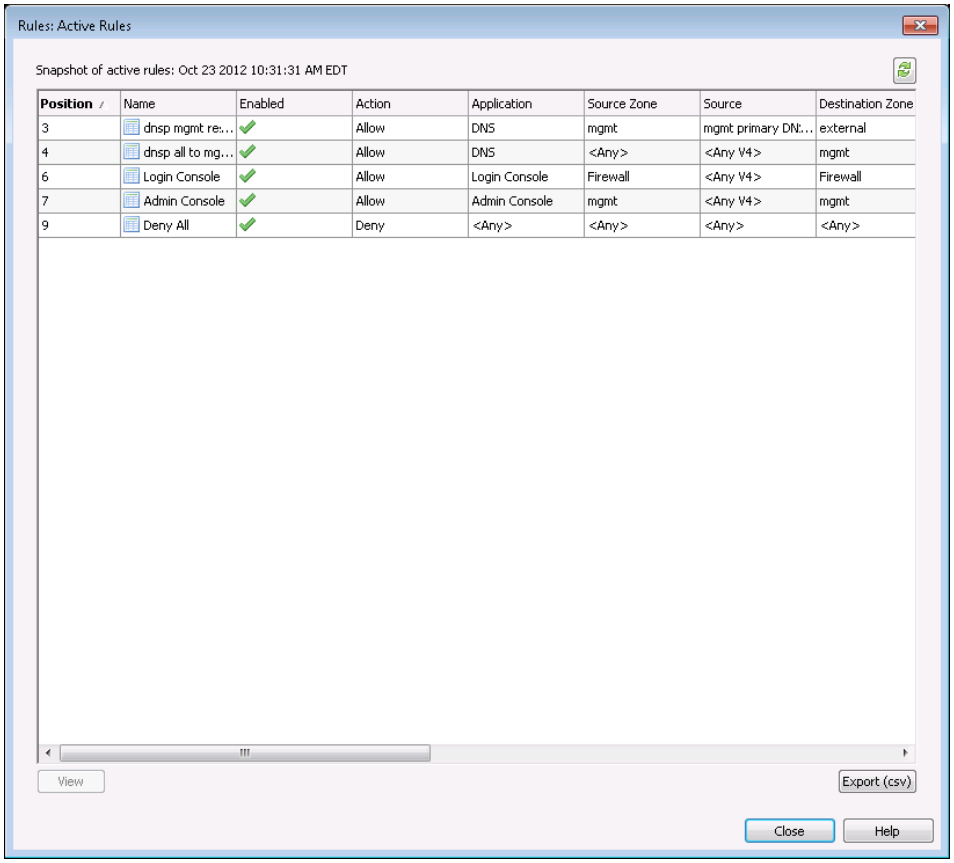


Figure 20 – Active Rules Popup

The process to enable Approved mode is provided below:

1. Under "**Policy/Application Defenses/ Defenses/HTTPS**", disable all non-Approved versions of SSL, leaving only TLS 1.0 operational.

2. Under "**Maintenance / Certificate Management**", ensure that the certificates only use Approved cryptographic algorithms.
3. Select "**Maintenance / FIPS**". The FIPS check box appears in the right pane (shown in Figure 21).
4. Select "**Enable FIPS 140-2 processing**".
5. Save the configuration change.
6. Select "**Maintenance / System Shutdown**" to reboot the firewall to the Operational kernel to activate the change.

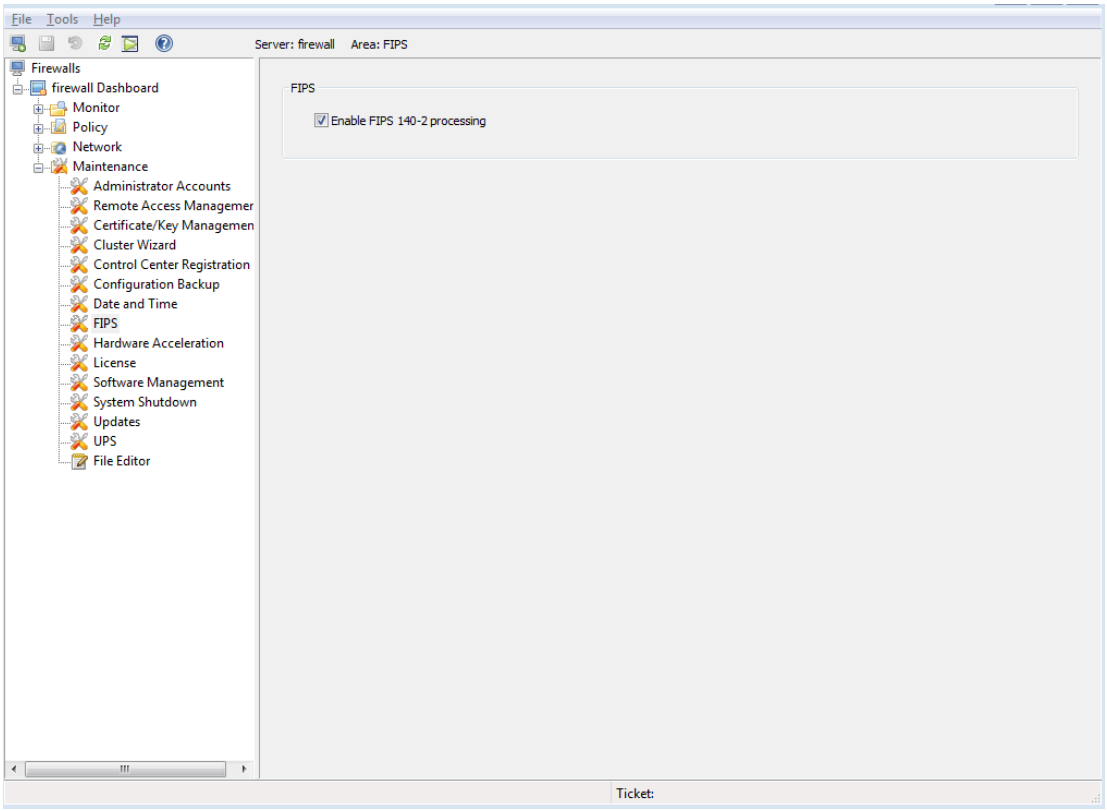


Figure 21 – Configuring For FIPS

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

- Firewall Authentication private key
- Local CA private key

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

3.1.2 Management

When configured according to the Crypto-Officer guidance in this Security Policy, the module only runs in an Approved mode of operation. While in Approved mode, only Approved and Allowed algorithms may be used; the use of non-Approved algorithms is prohibited. The Crypto-Officer is able to monitor and

configure the module via the web interface (GUI over TLS), SSH, serial port, or direct-connected keyboard/monitor. Detailed instructions to monitor and troubleshoot the systems are provided in the *McAfee Firewall Enterprise 8.3.0 Product Guide*. The CO must monitor that only Approved algorithms as listed in Table 2 above are being used for TLS, DTLS, and SSH sessions.

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

3.1.3 Physical Inspection

For the module to operate in its Approved mode, the tamper-evident seals must be placed by the CO role as specified in Section 3.1.1.1 above. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO is also responsible for the following:

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

The CO is also required to periodically inspect the module for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of malice. If evidence of tampering is found during periodic inspection, the Crypto-Officer must zeroize the keys and re-image the module before bringing it back into operation.

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

3.1.4 Monitoring Status

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

The "show status" service to determine the current mode of operation involves examining the Admin Console's FIPS mode checkbox, shown in Figure 21. This can also be done via the following CLI command:

```
cf fips query
```

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

```
fips set enabled=yes
```

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

The Crypto-Officer must monitor the module's status regularly for Approved mode of operation and active bypass mode. If any irregular activity is noticed or the module is consistently reporting errors, then McAfee customer support should be contacted.

3.1.5 Zeroization

It is the Crypto Officer's responsibility to zeroize the module's keys when necessary. In order to zeroize the module of all keys and CSPs, it is necessary to first rebuild the module's image, essentially wiping out

all data from the module. Once a factory reset has been performed, default keys and CSPs must be set up as part of the renewal process. These keys must be recreated as per the instructions found in section 3.1.1.4. Failure to recreate these keys will result in a non-compliant module.

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

3.2 User Guidance

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

3.3 Non-Approved Mode of Operation

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

4 Acronyms

This section describes the acronyms used throughout the document.

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BIOS	Basic Input/Output System
CAC	Common Access Card
CAST	Carlisle Adams and Stafford Tavares
CBC	Cipher-Block Chaining
CD	Compact Disc
CD-ROM	Compact Disc – Read-Only Memory
CE	Cryptographic Engine
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol

.

Acronym	Definition
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
KAT	Known Answer Test
KCLSOS	Kernel Cryptographic Library for SecureOS®
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MAC	Message Authentication Code
MD	Message Digest
MIB	Management Information Base
NAT	Network Address Translation
NIA	Network Integrity Agent
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMI	Non-Maskable Interrupt
NMS	Network Management System
OFB	Output Feedback
OS	Operating System
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus

.

Acronym	Definition
UTM	Unified Threat Management
VGA	Video Graphics Array
VPN	Virtual Private Network

Prepared by:
Corsec Security, Inc.

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

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