McAfee, Inc.

McAfee Web Gateway Virtual Appliance

Software Version: 7.3.2.3.4

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.4

Prepared for:

McAfee, Inc. Headquarters
2821 Mission College Blvd.
Santa Clara, CA 95054
United States of America

Phone: +1 (888) 847-8766
http://www.mcafee.com

Prepared by:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the McAfee Web Gateway Virtual Appliance from McAfee, Inc. This Security Policy describes how the McAfee Web Gateway Virtual Appliance 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 (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The McAfee Web Gateway Virtual Appliance is referred to in this document as McAfee Web Gateway, the virtual appliance, 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 Web Gateway Virtual Appliance

2.1 Overview

McAfee, Inc. is a global leader in Enterprise Security solutions. The company's comprehensive portfolio of network security products and solutions provides unmatched protection for the enterprise in the most mission-critical and sensitive environments.

The McAfee Web Gateway Virtual Appliance is a high-performance, enterprise-strength proxy appliance that provides the caching, authentication, administration, and authorization controls required by today's most demanding enterprises. The McAfee Web Gateway Virtual Appliance delivers deployment flexibility and performance, along with scalability to easily support hundreds of thousands of users in a single environment. McAfee Web Gateway Virtual Appliance delivers comprehensive security for all aspects of Web 2.0 traffic.

McAfee Web Gateway ensures comprehensive web security for networks. It protects networks against threats arising from the web, such as viruses and other malware, inappropriate content, data leaks, and related issues. It also ensures regulatory compliance and a productive work environment.

The virtual appliance is installed as a gateway that connects a network to the web. Following the implemented web security rules, it filters the requests that users send to the web from within the network. Responses sent back from the web and embedded objects sent with requests or responses are also filtered. Malicious and inappropriate content is blocked, while useful content is allowed to pass through.

Web filtering is accomplished via the following processes:

- Intercepting web traffic: this is achieved by the gateway functions of the virtual appliance, using different network protocols and services such as HTTP[1], HTTPS[2], FTP[3], Yahoo, ICQ, Windows Live Messenger, and others. As a gateway, the virtual appliance can run in explicit proxy mode or in transparent bridge or router mode.

- Filtering web objects: special anti-virus and anti-malware functions on the virtual appliance scan and filter web traffic and block objects when they are infected. Other functions filter requested URLs[4], using information from the global TrustedSource intelligence system, or do media type and HTML[5] filtering. They are supported by functions that do not filter themselves, but do tasks such as counting user requests or indicating the progress made in downloading web objects.

- Filtering users: this is done by the authentication mechanisms provided by the virtual appliance, using information from internal and external databases and methods such as NTLM[6,7,8], LDAP[9], RADIUS[10], Kerberos, and others. In addition to filtering normal users, the virtual appliance also provides control over administrator rights and responsibilities.

- Monitoring the filtering process: the monitoring functions of the appliance allow administrators a continuous overview of the filtering process. The monitoring functions include a dashboard,

[1] HTTP – Hypertext Transfer Protocol
[2] HTTPS – Secure Hypertext Transfer Protocol
[3] FTP – File Transfer Protocol
[4] URL – Uniform Resource Locator
[5] HTML – Hypertext Markup Language
[6] NTLM – Microsoft Windows NT LAN Manager
[7] NT – New Technology
[8] LAN – Local Area Network
[9] LDAP – Lightweight Directory Access Protocol
[10] RADIUS – Remote Authentication Dial-up User Service

which provides information on web usage, filtering activities, and system behavior. The dashboard also provides logging and tracing functions and options to forward data to an ePolicy Orchestrator. Event monitoring is provided by an SNMP[11] agent.

For user-initiated web requests, McAfee Web Gateway first enforces an organization's internet use policy. For all allowed traffic, it then uses local and global techniques to analyze the nature and intent of all content and active code entering the network via the requested web pages, providing immediate protection against malware and other hidden threats. Additionally, the SSL[12] Scanner feature of McAfee Web Gateway can examine TLS[13] traffic to provide in-depth protection against malicious code that might otherwise be disguised through encryption.

To secure outbound traffic, McAfee Web Gateway scans user-generated content on all key web protocols, including HTTP, HTTPS, and FTP. As part of a fully-integrated McAfee data loss prevention solution, McAfee Web Gateway protects against loss of confidential information and other threats leaking from the organization through blogs, wikis, and online productivity tools such as organizers and calendars.

The McAfee Web Gateway Virtual Appliance also provides administrators with the ability to monitor and troubleshoot the appliance.

McAfee Web Gateway combines and integrates numerous protections that would otherwise require multiple stand-alone products. Web filtering, anti-virus, anti-spyware, SSL scanning, and content control filtering capabilities are combined into a single virtual appliance. A simplified management footprint means that a single compliance policy can be shared across protections and protocols. A sample deployment scenario is diagramed in Figure 1.

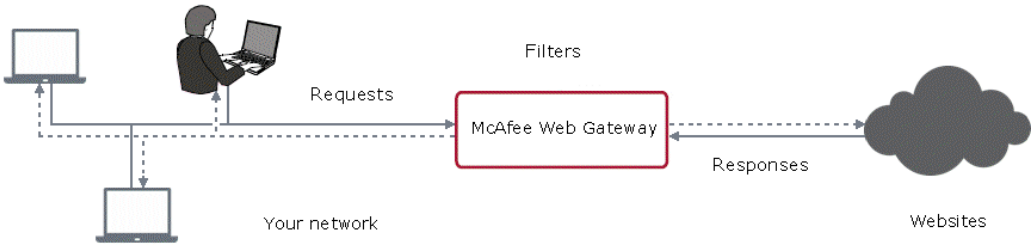

Figure 1 – Typical Deployment Scenario

The McAfee Web Gateway Virtual Appliance is validated at the FIPS 140-2 Section levels shown in Table 1 below.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1

[11] SNMP – Simple Network Management Protocol
[12] SSL – Secure Sockets Layer
[13] TLS – Transport Layer Security

Section	Section Title	Level
5	Physical Security	N/A[14]
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[15]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The McAfee Web Gateway Virtual Appliance is a multi-chip standalone cryptographic software module that meets overall Level 1 FIPS 140-2 requirements. The cryptographic boundary of McAfee Web Gateway consists of McAfee Web Gateway application software, a cryptographic library and McAfee's own McAfee Linux Operating System (MLOS) v2.2.3. The cryptographic boundary is shown by the red-colored, dotted line in Figure 2. It is designed to execute on a General Purpose Operating System running a VMware hypervisor. As a virtual appliance, McAfee Web Gateway must be installed on a supported virtual machine hypervisor. The module was tested and found compliant on an Intel SR2625URLX Server System running the ESXi hypervisor provided by VMware vSphere 5.0.

2.2.1 Physical Cryptographic Boundary

As a software cryptographic module, there are no physical protection mechanisms implemented. Therefore, the module must rely on the physical characteristics of the host system. The physical boundary of the cryptographic module, running within a virtual environment, is defined by the hard enclosure of the host system on which it runs, as shown by the red-colored dotted line in Figure 2. The module supports the physical interfaces of the host device, which directly hosts the virtual environment the module has been installed on. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM, hard disk, device case, power supply, and fans. See Figure 2 for a diagram of the typical host device.

[14] N/A – Not Applicable
[15] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

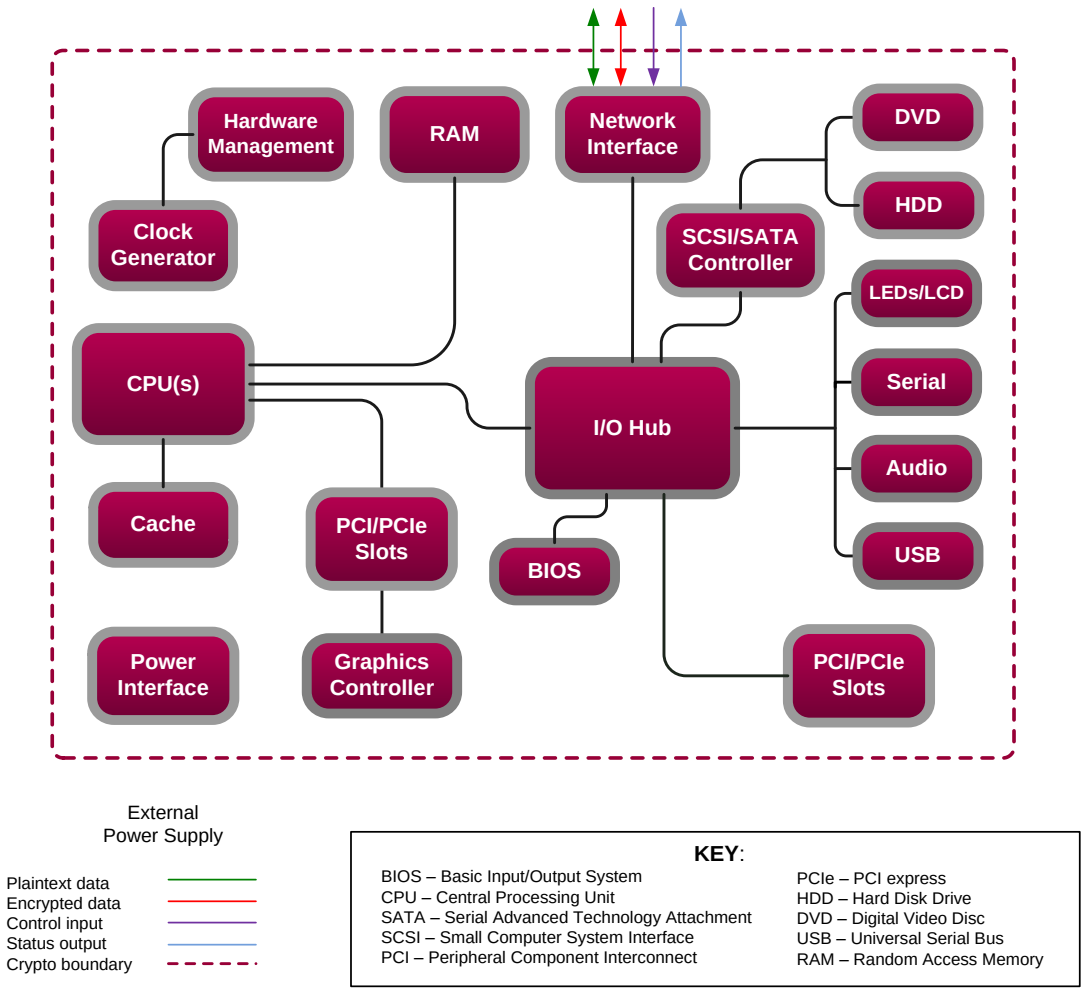

Figure 2 – GPC Block Diagram

2.2.2 Logical Cryptographic Boundary

The module is considered to be a software cryptographic module. Therefore the module has a logical cryptographic boundary in addition to a physical cryptographic boundary. The logical cryptographic boundary of the module consists of the McAfee Web Gateway Virtual Appliance running MLOS v2.2.3. Figure 3 shows the logical block diagram (red-dotted line) of the module executing in memory and its interactions with the VMware vSphere hypervisor through the module's defined logical cryptographic boundary. The module interacts directly with the hypervisor, which runs directly on the host system. The hypervisor controls and directs all interactions between McAfee Web Gateway and the operator.

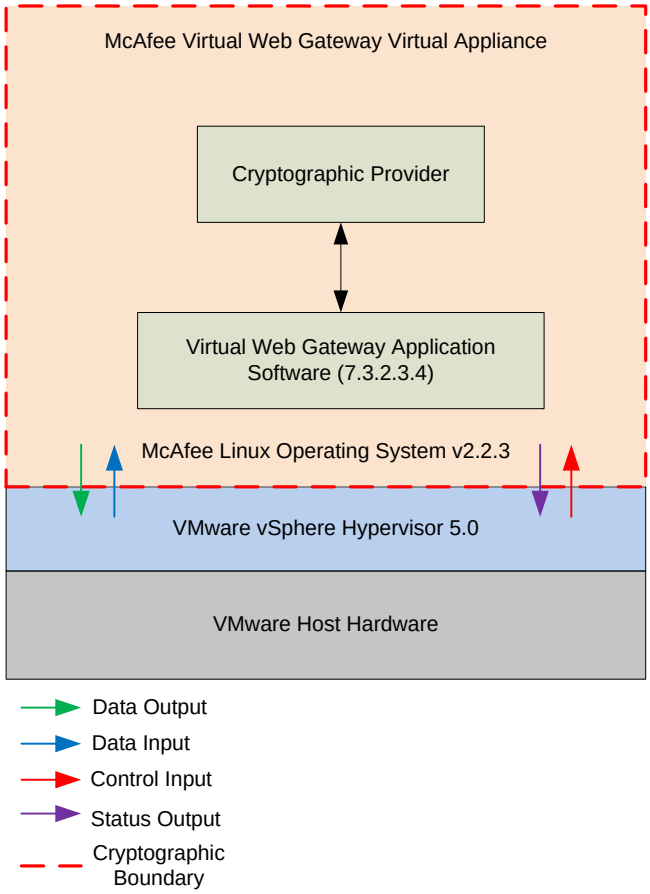

Figure 3 – McAfee Web Gateway Logical Cryptographic Boundary

2.3 Module Interfaces

The McAfee Web Gateway Virtual Appliance is a multi-chip standalone cryptographic module that meets overall Level 1 FIPS 140-2 requirements. 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

As a software module, the virtual appliance has no physical characteristics. The module's physical and electrical characteristics, manual controls, and physical indicators are those of the host system. The VMware hypervisor provides virtualized ports and interfaces for the module. Interaction of with the virtual ports created by the hypervisor occurs through the host system's Ethernet port. Management, data, and status traffic must all flow through the Ethernet port. Direct interaction with the module via the host system is not possible. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 2 below.

Table 2 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Logical Port/Interface	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet Ports, Virtual USB Ports, Virtual Serial Ports	• Data Input • Data Output • Control Input • Status Output

Data input and output are the packets utilizing the services provided by the modules. These packets enter and exit the module through the Virtual Ethernet ports. Control input consists of Configuration or Administrative data entered into the modules. Status output consists of the status provided or displayed via the user interfaces (such as GUI or CLI) or available log information.

2.4 Roles and Services

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

2.4.1 Cryptographic 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 the following management interfaces to the CO:

- MWGUI[16]
- SNMPv3

2.4.2 User Role

A User of the module is any one of a set of clustered modules that share configuration information of the master McAfee Web Gateway Virtual Appliance. Users have to authenticate to the module with a valid certificate before they can access any of the user services. See section 2.4.5 below.

2.4.3 Services

Services provided to authenticated operators are provided in Table 3 below. Please note that the keys and Critical Security Parameters (CSPs) listed indicate the type of access required:

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

[16] MWGUI – McAfee Web Gateway Graphical User Interface

Table 3 – Authenticated Services

Service	Description	Operator		Approved Algorithms Accessed	Type of Access
		CO	User		
Perform initial configuration	Configure the primary network interface, IP[17] address, host name, and DNS[18] server	X		N/A	None
CO Login	Crypto-Officer login	X		AES, Triple-DES, RSA, SHA, HMAC, SP 800-90A DRBG	DH[19] Establishment Public Key – RX; DH Establishment Private Key – RX; RSA[20] Establishment Public Key – WRX; RSA Establishment Private Key – WRX; TLS Session Key – RWX; MWGUI Public Key – RX; MWGUI Private Key – RX; CO password – RX
Implement/modify a web security policy*	Create/modify web security policy using rules and filter lists	X		RSA	Root CA[21] Private Key – RW; Root CA Public Key – RW; RADIUS shared secret – WX; LDAP account password – WX; NTLM machine account password – WX
Import a license*	Import a license	X		N/A	None
Modify configuration settings*	Modify virtual appliance configuration settings	X		RSA	MWGUI Public Key – WX; MWGUI Private Key – WX; Cluster CA Public Key – WX; Cluster server key – WX; Cluster client key – WX; WCCP[22] authentication key – WX; SNMP v3 passwords – WX; NTLM machine account password – WX SWPS key – WX;
Manage administrator account*	Set up account for administrator	X		N/A	CO password – WX; RADIUS shared secret – WX; NTLM machine account password – WX; SNMP v3 passwords – WX;

[17] IP – Internet Protocol
[18] DNS – Domain Name System
[19] DH – Diffie Hellman
[20] RSA – Rivest, Shamir, and Adleman
[21] CA – Certificate Authority
[22] WCCP – Web Cache Communication Protocol

Service	Description	Operator		Approved Algorithms Accessed	Type of Access
		CO	User		
Backup appliance configuration*	Store the virtual appliance's configuration information (including rules, lists, settings, and administrator accounts) in a backup file	X		RSA	CO Password – X; SNMP v3 Password – X; RADIUS shared secret – X; LDAP account password – X; MWGUI Public Key – X; MWGUI Private Key – X; Root CA Private Key – RW; Root CA Public Key – RW; WCCP key – R
Restore appliance configuration*	Restore the virtual appliance's configuration information from a backup file	X		RSA	CO Password, SNMP v3 Password, RADIUS shared secret, LDAP account password, MWGUI Public Key, MWGUI Private Key, Root CA Private key, Root CA Public key, WCCP key – WX
Monitor system functions*	Monitor how the virtual appliance executes its filtering functions	X		N/A	None
Monitor status on SNMP	Monitors non security relevant status of the module via SNMPv3	X		N/A	SNMP v3 Password -RX
Perform self-tests*	Run self-tests on demand (via MWGUI)	X		N/A	None
Perform self-tests	Run self-tests on demand (via power cycle)	X		N/A	None
Show status*	Allows Crypto-Officer to check module status	X		N/A	None
Zeroize	Zeroizes the module to the factory default state	X		N/A	All Keys and CSPs – W
Configure cluster CA*	Services required to communicate with each other in multi-appliance configurations	X		RSA	Cluster CA Public Key – W; Cluster server key – W; Cluster client key – W
Management over REST[23] *	Shutdown or restart the virtual machine; view log files; flush the cache; create configuration backup	X		N/A	CO Password – X
Note: The '*' above indicates the 'CO Login' service is required.					

[23] REST – Representational State Transfer

Service	Description	Operator		Approved Algorithms Accessed	Type of Access
		CO	User		
Configuration sharing	Clustered instances share the configuration information of the McAfee Web Gateway master		X	AES, Triple-DES, RSA, SHA, HMAC, SP 800-90A DRBG	DH Establishment Keys – RWX; Cluster CA Public Key – RX; Cluster server key – RX; Cluster client key – RX; TLS session key – WX; CO Password, SNMP v3 Password, RADIUS shared secret, LDAP account password, MWGUI Public Key, MWGUI Private Key , Root CA Private Key, Root CA Public Key, WCCP – WR (depending on originator)

2.4.4 Non-Security Relevant Services

In addition to the services listed in Table 3, the modules provide non-security relevant services. All services provided by the modules are provided in the modules' product guide*: McAfee Web Gateway 7.3.2: Product Guide; Revision A (2013)*. The document is publicly available for download at:

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24502/en_US/mwg_732_pg_product_a_en-us.pdf.

2.4.5 Authentication Mechanisms

Crypto-Officers may authenticate to the module over the MWGUI with a combination of username and password or with a client certificate.

Users may authenticate to the module using one of the following configurable methods:

- NTLM
- NTLM-Agent
- LDAP
- RADIUS
- SWPS[24]
- Kerberos

The modules supports role-based authentication. An operator explicitly assumes either a Crypto-Officer role or a User role based on the authentication credentials. Please refer to the Table 4 for the authentication methods used by operators to authenticate to the module and assume an authorized role.

[24] SWPS – Secure Web Protection Service

Table 4 – 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 1,000 characters. The password must contain the following: • At least one lower case letter. • At least one upper case letter. • At least one numeric or special character. Starting with all 8-character strings: 95^8 Then remove all passwords with no lowercase (69^8), all passwords with no uppercase (69^8), and all passwords with no digits/specials (52^8). But then you removed some passwords twice. You must add back all passwords with: • no lowercase and no uppercase: 43^8 • no lowercase and no digits/specials: 26^8 • no uppercase and no digits/specials: 26^8 $95^8 - 69^8 - 69^8 - 52^8 + 43^8 + 26^8 + 26^8 =$ $5{,}565{,}253{,}689{,}908{,}640 \approx 5.565 \times 10^{15}$ passwords The chance of a random attempt falsely succeeding is 1: 5.565×10^{15}.
Crypto-Officer/ User	RSA Public Key Certificate	The module supports RSA digital certificate authentication during TLS sessions. Using conservative estimates and equating a 2048-bit RSA key to an 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$.
Crypto-Officer	One Time Password	When enabled, a one-time password is sent to the CO after successfully authenticating with an RSA digital certificate. The CO must type in the received password in order to authenticate to the module. The use of a one-time password acts as a two-factor authentication method, which greatly increases the overall strength of CO's password.

2.5 Physical Security

McAfee Web Gateway Virtual Appliance is a software module, which FIPS defines as a multi-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The operational environment for the module consists of MLOS v2.2.3 and the VMware hypervisor. The module was tested and found to be compliant with FIPS 140-2 requirements on hypervisors provided by VMware vSphere 5.0 running on an Intel SR2625URLX Server System. All cryptographic keys and CSPs are under the control of MLOS v2.2.3 and the hypervisor, which protect the CSPs against unauthorized disclosure, modification, and substitution.

2.7 Cryptographic Key Management

The module's cryptographic functionality is provided by a software library that offers secure networking protocols and cryptographic functionalities. Security functions offered by the module map to the certificates listed in Table 5.

Table 5 – Algorithm Certificate Numbers for Cryptographic Libraries

Approved Security Function	CVL Certificate Number
Symmetric Key Algorithm	
AES[25]: 128-, 192-, 256-bit in CBC[26] mode	3117
Triple-DES[27] : 168-bit in CBC mode	1788
Secure Hashing Algorithm (SHA)	
SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	2573
Message Authentication Code (MAC) Function	
HMAC[28] using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	1954
Deterministic Random Bit Generator (DRBG)	
SP800-90A CTR_DRBG	628
Asymmetric Key Algorithm	
RSA[29] Key Pair Generation (FIPS 186-4) with 2048- bit keys	1588
RSA PKCS[30] #1 v1.5 Signature Generation (FIPS 186-4) with 2048-bit keys	1588
RSA PKCS #1 v1.5 Signature Verification (FIPS 186-2) with 1024-, 1536-, 2048-, 3072-, 4096-bit keys	1588
Digital Signature Algorithm (DSA) signature verification: 1024-bit	901

Additional information concerning SHA-1, RSA key signatures, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The cryptographic module implements the TLS and SNMP secure networking protocols. Each protocol implements a Key Derivation Function (KDF) listed in NIST SP 800-135rev1 and has been validated by

[25] AES – Advanced Encryption Standard
[26] CBC – Cipher-Block Chaining
[27] DES – Data Encryption Standard
[28] HMAC – (Keyed-) Hash Message Authentication Code
[29] RSA – Rivest, Shamir, Adleman
[30] PKCS – Public Key Cryptography Standards

the CMVP. There certificate numbers are provided in Table 6. The complete protocol implementations have not been reviewed or tested by the CAVP[31] and CMVP.

Table 6 – Network Protocol Component Validation

Algorithm	Certificate Number
TLS 1.0/1.1 and TLS 1.2 KDF[32] using SHA 256 and SHA 384	379
SNMP KDF using SHA-1	379

The module implements the following non-compliant key establishment methodologies:

- Diffie-Hellman: 2048-bit key (key agreement; key establishment methodology provides 112 bits of encryption strength)
- RSA: 2048-bit keys (key wrapping; key establishment methodology provides 112 bits of encryption strength)

The module employs a non-Approved Non-Deterministic Random Number Generator (NDRNG), which is used as an entropy source for seeding the Approved DRBG listed in Table 5. Its use is allowed per FIPS 140-2 Implementation Guidance 7.11.

[31] CAVP – Cryptographic Algorithm Validation Program
[32] KDF – Key Derivation Function

The module supports the CSPs listed below in Table 7.

Table 7 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Crypto-Officer Password	Password	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored as SHA256 hash in the configuration on hard disk	Overwritten by another password or when appliance is re-imaged	Authentication of administrators (Crypto-Officers)
SNMP v3 Password	Password	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored as USM[33] hash (rfc3414) in the configuration on hard disk	Overwritten by another password or when appliance is re-imaged	Used with SHA-1 and AES for authentication of SNMP requests
RADIUS Shared Secret	Password	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored in plain text in the configuration on hard disk	Overwritten by another password or when appliance is re-imaged	Authenticate RADIUS messages
NTLM Account Password	Password	Internally generated by FIPS approved DRBG	Never leaves the module	Stored on hard disk in plain text	Overwritten by another password or when appliance is re-imaged	Authenticate at Domain
LDAP Account Password	Password	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored on hard disk in plain text in the configuration	Overwritten by another password or when appliance is re-imaged	Authenticate at LDAP
Kerberos Password	Password	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored in plain text in the configuration on hard disk	Overwritten by another password or when virtual machine is reinstalled	Authenticate Kerberos messages
Cluster CA Public Key	X509 / RSA >= 2048 bits	Preinstalled and later changed via MWGUI	Leaves the module in plaintext	Stored on hard disk in plain text	Overwritten via MWGUI or when appliance is re-imaged	Verification of other cluster member and issuing of a cluster client certificate

[33] USM – User-based Security Model

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SWPS Key	Pre-shared key	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored in plain text in the configuration on hard disk	Overwritten via MWGUI or when appliance is re-imaged	End User authentication over encrypted channel
Cluster Communication Private Key	RSA private key with 2048 bits	Internally generated by FIPS approved DRBG	Private key will not leave the module	Stored on hard disk in plain text	Appliance re-image or reissuing due to Cluster CA change	Client / Server authentication for Transport Layer Security cluster communication
Cluster Communication Public Key	X509 / RSA public key with 2048 bits	Internally generated by following FIPS 186-4	Leaves the module in plaintext	Stored on hard disk in plain text	Appliance re-image or reissuing due to Cluster CA change	Client / Server authentication for TLS cluster communication
MWGUI Private Key	RSA private key with 2048 bits	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored in plain text in the configuration on hard disk	Overwritten via MWGUI or when appliance is re-imaged	Serve TLS connection to the MWGUI
MWGUI Public Key	X509, RSA public key with 2048 bits	Set via MWGUI or imported	Configuration sharing or backup – encrypted; Leaves the module in plaintext	Stored in plain text in the configuration on hard disk	Overwritten via MWGUI or when appliance is re-imaged	Serve TLS connection to the MWGUI
Root CA Private Key	RSA private key with 2048 bits	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored in plain text in the configuration file on hard disk	Overwritten via MWGUI or when appliance is re-imaged	SSL-Scanner: Issuing server certificates
Root CA Public Key	X509, RSA public key with 2048 bits	Set via MWGUI or imported	Configuration sharing or backup – encrypted; Leaves the module in plaintext	Stored in plain text in the configuration on hard disk	Overwritten via MWGUI or when appliance is re-imaged	SSL-Scanner: Verification of TLS connections
DH Establishment Private Key	Diffie-Hellman private key 224-bit	Internally generated by FIPS approved DRBG	Never leaves the module	Stored in plain text on hard disk	By power cycle or session termination	TLS connections for cluster communication, configuration, signature updates and SSL Scanner functions

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DH Establishment Public Key	Diffie-Hellman Public key 2048-bit	Generated externally; Preinstalled	Leaves the module in plaintext	Stored in plain text on hard disk	By power cycle or session termination	TLS connections for cluster communication, configuration, signature updates and SSL Scanner functions
RSA Key Establishment Private Key	RSA private key 2048-bit	Internally generated by following FIPS 186-4	Never leaves the module	Stored in plain text on hard disk	By power cycle or session termination	TLS connections for MWGUI or SSL Scanner
RSA Key Establishment Public Key	RSA public key 2048-bit	Internally generated by following FIPS 186-4	Leaves the module in plaintext	Stored in plain text on hard disk	By power cycle or session termination	TLS connections for MWGUI or SSL Scanner
TLS Session Key	Triple-DES, AES 128, AES 256	Internally generated by the TLS KDF	Output in encrypted form during TLS handshake	Volatile memory in plain text	By power cycle or session termination	TLS connections for cluster communication, Configuration, signature updates and SSL Scanner functions
DRBG Seed	Random data	Internally Generated	Never	Not persistently stored by the module	By power cycle; DRBG uninstantiation	Seeding material for SP 800-90A DRBG
DRBG Entropy	Random data (512 - 75203 Bytes)	Internally Generated	Never	Not persistently stored by the module	By power cycle; DRBG uninstantiation	Entropy material for SP 800-90A DRBG
DRBG 'V' Value	Internal state value	Internally Generated	Never	Not persistently stored by the module	By power cycle; DRBG uninstantiation	Secret, internal value for the CTR_DRBG
DRBG 'Key' Value	Internal state value	Internally Generated	Never	Not persistently stored by the module	By power cycle; DRBG uninstantiation	Key used for generating random material by the CTR_DRBG

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
WCCP Authentication Key	Password	Set via MWGUI or imported	Configuration sharing or backup – encrypted	Stored in plain text in the configuration on hard disk	Overwritten by another password or when appliance is re-imaged	Authentication (MD5) for WCCP UDP[34] control packets

2.8 Self-Tests

McAfee Web Gateway performs power-up and conditional self-tests as stated in the sections below.

2.8.1 Power-Up Self-Tests

McAfee Web Gateway performs the following self-tests at power-up:

- Software integrity check using a HMAC-SHA-256 hash
- Known Answer Tests (KAT)
  - AES Encrypt KAT
  - AES Decrypt KAT
  - Triple-DES Encrypt KAT
  - Triple-DES Decrypt KAT
  - SHA-1 KAT
  - HMAC KAT with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
  - RSA Signature Generation KAT
  - RSA Signature Verification KAT
  - RSA Key Wrap KAT
  - RSA Key Unwrap KAT
  - SP 800-90A CTR_DRBG KAT
- DSA Pairwise Consistency Test (verify operation)

If any of the tests listed above fail to perform successfully, the module enters a critical error state where all cryptographic operations and output of any data is prohibited. Operators can reboot the virtual appliance to clear the error and resume normal operation.

2.8.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for SP 800-90A CTR_DRBG
- Continuous RNG Tests for NDRNG
- RSA pairwise consistency test (for sign and verify operations)

If any of the tests listed above fail to perform successfully, the module enters a critical error state where all cryptographic operations and output of any data is prohibited. Operators can reboot the virtual appliance to clear the error and resume normal operation.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

[34] UDP – User Datagram Protocol

3 Secure Operation

The McAfee Web Gateway Virtual Appliance meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in operation.

3.1 Initial Setup

The following sections provide step-by-step instructions necessary to configure the module for operation. For any questions or issues that arise at any point during the installation and configuration of the virtual appliance, contact the McAfee support team at http://www.mcafee.com/us/support.aspx. Documents mentioned in these instructions are freely available at the following web address: http://kc.mcafee.com.

3.1.1 Setting FIPS Environment

In order to setup the virtual appliance in the validated configuration, the following steps will need to be performed by the Crypto-Officer:

1. Obtain version 7.3.2.3.4 installation image from McAfee's Content & Cloud Security Portal.
2. Open a virtual machine management client and create a new virtual machine on the hypervisor.
    a. Please refer to the *McAfee Web Gateway 7.3.2 Product Guide* for minimum environmental requirements
3. When asked to provide an *.iso[35] file, provide the image obtained in step one.
4. Start the virtual machine.
5. When presented with the Installer interface, select option #5 – "Install Appliance in FIPS mode"
6. Follow the procedures included in the Installation Guide to complete installation using the installation wizard. The module will reboot.
7. After successful installation, please ensure that the following features are turned off:
    1) The log file encryption and/or anonymization feature must be turned off
        a) Confirm the "Encrypt the log file" flag under the Policy>Settings>File System Logging>Access Denied Log Configuration tab is not enabled
        b) Confirm that nothing appears when searching for the "FileSystemLogging.MakeAnonymous" property
8. Reboot the module.

The appliance is now considered to be in its validated configuration.

3.2 Crypto-Officer Guidance

The Crypto-Officer is responsible for initializing the module, performing security-relevant configuration, and monitoring the module. During initial set up, the CO shall change the default admin password, MWGUI server certificate, and the cluster CA. Additionally, the CO shall ensure that the log file encryption and/or anonymization feature is turned off when the module is being operated.

The Crypto-Officer can initiate the execution of self-tests, and can access the module's status reporting capability. Self-tests can be initiated at any time by restarting the virtual appliance.

3.2.1 Management

The Crypto-Officer is responsible for maintaining and monitoring the status of the module. Please refer to Section 3.1 above for guidance that the Crypto-Officer must follow. To obtain the current FIPS status of the module, the CO should access the module via the MWGUI. On the upper, left-hand corner of the GUI, the CO will see "FIPS 140-2" when the module has been properly configured.

[35] ISO – International Organization for Standardization

For details regarding the management of the module, please refer to the McAfee Web Gateway Installation Guide.

3.2.2 Zeroization

Session keys are zeroized at the termination of the session, and are also cleared when the module is power-cycled. Zeroizartion also includes the SP 800-90A CTR_DRBG seed, entropy, and key values. All other CSPs may be zeroized by reinstalling the virtual appliance. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

3.3 User Guidance

The User does not have the ability to configure sensitive information on the module.

4 Acronyms

Table 8 in this section describes the acronyms used throughout the document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Digital Encryption Standard
DNS	Domain Name System
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
ISO	International Organization for Standardization
MD	Message Digest
HMAC	(Keyed-) Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MD	Message Digest

Acronym	Definition
MLOS	McAfee Linux Operating System
MWGUI	McAfee Web Gateway Graphical User Interface
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NT	New Technology
NTLM	Microsoft Windows NT LAN Manager
OS	Operating System
PKCS	Public Key Cryptography Standard
RADIUS	Remote Authentication Dial-In User Service
RC	Rivest Cipher
REST	Representational State Transfer
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SWPS	Secure Web Protection Service
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USM	User-based Security Model
UUID	Universally Unique Identifier
WCCP	Web Cache Communication Protocol

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