McAfee, Inc.

McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances

Hardware Models: WBG-5000-C, WBG-5500-C; Firmware Version: 7.3.2.3.4

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.5

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.
13921 Park Center Road, Suite 460
Herndon, VA 20171
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 WBG-5000-C and WBG-5500-C Appliances from McAfee, Inc. This Security Policy describes how the McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances 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 (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 WBG-5000-C and WBG-5500-C Appliances are referred to in this document collectively as the McAfee Web Gateway, the appliance, 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 McAfee Web Gateway WBG-5000-C and WBG-5500-C 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 Web Gateway is a high-performance, enterprise-strength proxy appliance family that provides the caching, authentication, administration, and authorization controls required by today's most demanding enterprises. With multiple appliance models to choose from, the McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances deliver deployment flexibility and performance, along with scalability to easily support hundreds of thousands of users in a single environment. McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances deliver comprehensive security for all aspects of Web 2.0 traffic. A view of the Model WBG-5000-C and WBG-5500-C is shown in Figure 1 and Figure 2 below.

Figure 1 – McAfee Web Gateway WBG-5000-C

Figure 2 – McAfee Web Gateway WBG-5500-C

The 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 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 appliance processes:

- Intercepting web traffic: this is achieved by the gateway functions of the 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 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 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 jobs 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 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 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, which provides information on web usage, filtering activities, and system behavior as 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, the 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 the 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, the 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, the 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 WBG-5000-C and WBG-5500-C Appliances also provide administrators with the ability to monitor and troubleshoot the appliance.

The 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 appliance. A simplified management footprint means that a single compliance policy can be shared across protections and protocols. Figure 3 shows a typical deployment scenario for the McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances.

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

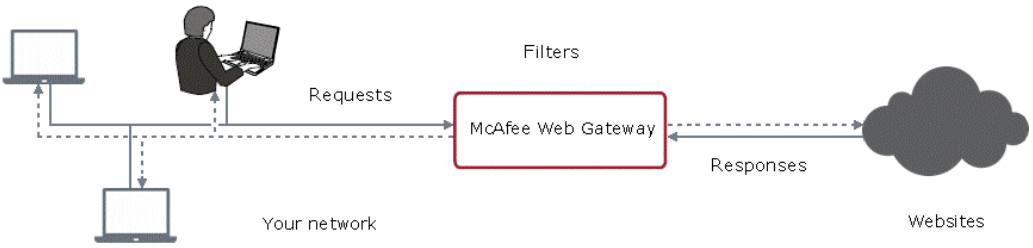

Figure 3 – Typical Deployment Scenario

Table 1 below provides general specification for the McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances.

Table 1 – McAfee Web Gateway Model Specifications

	WBG-5000-C	WBG-5500-C
Form Factor	1U rack-mount	1U rack-mount
Processor	Intel Xeon E5-2430 (1x 6-core)	Intel Xeon E5-2680V2 (2x 10-core)
Memory	16 GB	16 GB
Interfaces	4 x 10/100/1000	4 x 10/100/1000
RAID[14]	RAID 1/10	RAID 1/10
Hard Disk	Available: 8 x SAS Installed : 2 x 600 GB SAS	Available: 8 x SAS Installed : 6 x 300 GB SAS
Power Supply	Redundant	Redundant

The McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances are validated at the FIPS 140-2 Section levels shown in Table 2 below.

Table 2 – 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
5	Physical Security	1
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[15]	1

[14] RAID – Redundant Array of Inexpensive Disks

Section	Section Title	Level
9	Self-tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A[16]

2.2 Module Specification

The McAfee Web Gateway is a multi-chip standalone cryptographic hardware module that meets overall Level 1 FIPS 140-2 requirements. The cryptographic boundary of the module is defined by the hard metal chassis, which surrounds all the hardware and firmware components. Figure 4 depicts the block diagram and the cryptographic boundary of the module, which is indicated using the red dotted line. Please note that the anti-virus and URL categorization modules are excluded from the cryptographic boundary.

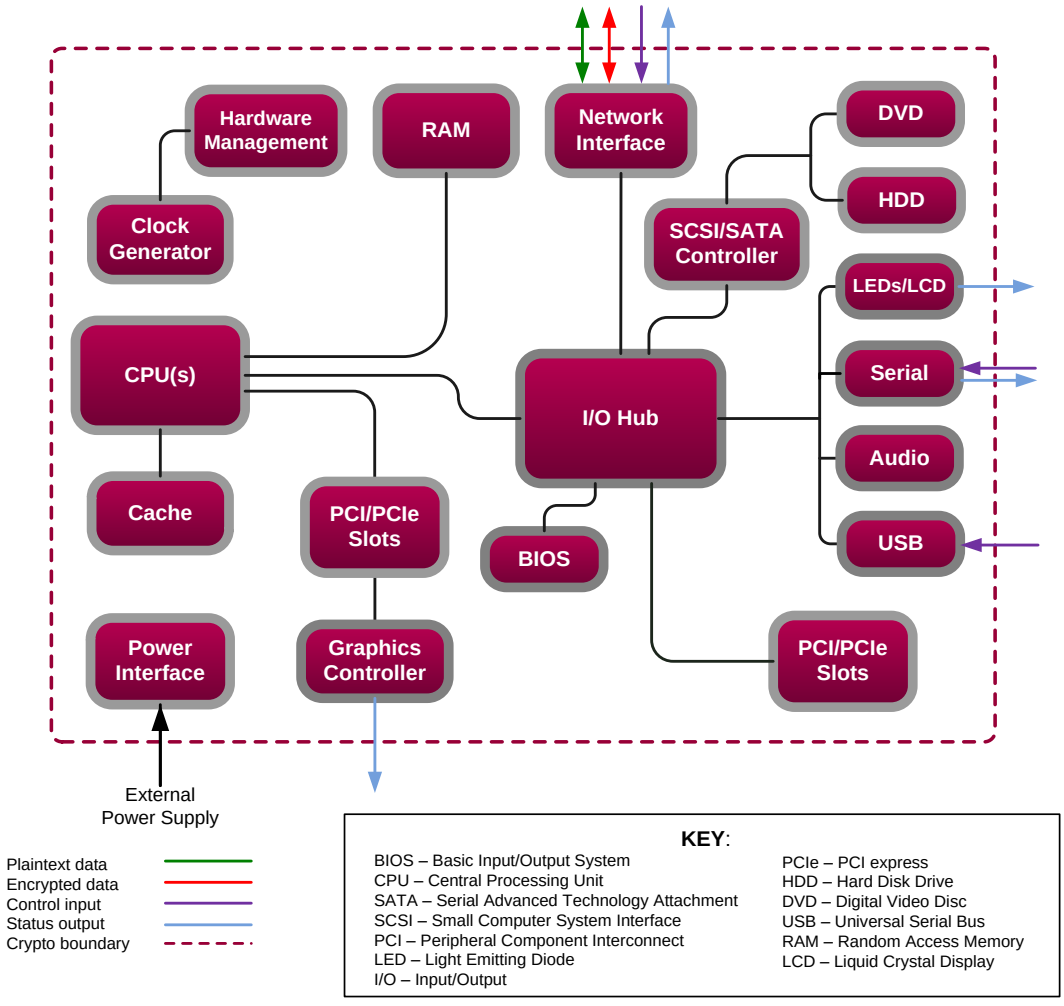

Figure 4 – Block Diagram for the WBG-5000-C and WBG-5500-C[17]

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

2.3 Module Interfaces

The McAfee Web Gateway 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

All ports and interfaces are located at the back side of the hardware module. The front of the chassis is populated with the power/sleep, reset, ID[18], and NMI[19] buttons, a USB port, and several LEDs[20]; please note that some of these are covered by the security bezel. The front and rear view of the appliances are shown in the figures below.

Figure 5 – McAfee Web Gateway WBG-5000-C (Front View)

Figure 6 – McAfee Web Gateway WBG-5500-C (Front View)

Figure 7 – McAfee Web Gateway WBG-5000-C (Rear View)

[17] It should be noted that either the serial port or the Graphics Controller (VGA) port is used for status output but not both at the same time.
[18] ID – Identification
[19] NMI – Non-Maskable Interrupt
[20] LED – Light-Emitting Diode

Figure 8 – McAfee Web Gateway WBG-5500-C (Rear View)

Table 3 below describes the ports and interfaces found on the two models of the cryptographic module.

Table 3 – McAfee Web Gateway Ports and Interfaces

Model	Physical Ports
Web Gateway WBG-5000-C	• CD-ROM Drive (covered by bezel) • Four (4) gigabit Ethernet ports • Four (4) USB ports • Two (2) USB ports (covered by bezel) • One (1) Intel RMM4[21] NIC[22] Port • One (1) serial port • One (1) Video Graphics Array (VGA) port • LEDs – System ID, System Status, Power, NIC (x4), Hard Disk • One (1) Intel® I/O module • Two (2) power connectors
Web Gateway WBG-5500-C	• Four (4) gigabit Ethernet ports • Three (3) Universal Serial Bus (USB) ports • One (1) Intel RMM4 NIC Port • One (1) serial ports • One (1) Video Graphics Array (VGA) port • LEDs – NIC (x4), Power, System Status, System ID, Hard Disk • One (1) Intel I/O module • Two (2) power connectors

Once the module has been mounted by the Crypto-Officer (CO), all physical ports marked with "(covered by bezel)" will not be accessible unless the bezel is removed by the Crypto-Officer. The Crypto-Officer role is defined in Section 2.4.1.

The module's ports and interfaces are mapped to logical interfaces in Table 4 below. All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 4.

Table 4 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Interface	McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances Physical Ports
Data Input	Ethernet ports

[21] RMM – Remote Management Module
[22] NIC – Network Interface Card

FIPS 140-2 Interface	McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances Physical Ports
Data Output	Ethernet ports
Control Input	Ethernet ports
Status Output	Ethernet ports, serial port, VGA port, LEDs
Power	Power connectors

Status output will be provided via the serial port or the VGA port, dependant on the option selected during installation of the v7.3.2.3.4 firmware. The USB and RMM4 ports are disabled once the module is configured.

Table 5 below provides a description of the LEDs visible on the WBG-5000-C and WBG-5500-C appliances with the bezels attached.

Table 5 – LED Descriptions

LED	Color	Condition	Description
Power/Sleep	Green	On	System on
		Blink[23,24]	Sleep
	Off	Off	System off
NIC 1-4	Green	On	NIC link
		Blink	NIC activity
System Status (on standby power)	Green	On	Running/ Normal Operation
		Blink[25]	Degraded
	Amber	On	Critical or non-recoverable condition
		Blink	Non-critical condition
	Off	Off	POST[26]/System Stop
Disk Activity	Green	Random blink	Provides an indicator for disk activity
	Off	Off[27]	No hard disk activity
System Identification	Blue	On	Identify active via command or button
	Off	Off	No identification

[23] Blink rate is ~1Hz at 50% duty cycle

[24] The power LED sleep indication is maintained on standby by the chipset. If the system is powered down without going through the BIOS, the LED state that is in effect at the time of power-off is restored when the system is powered on until the BIOS clears it. If the system is not powered down normally, it is possible that the power LED is blinking while the system status LED is off. This is due to a failure or configuration change that prevents the BIOS from running.

[25] The amber status takes precedence over the green status. When the amber LED is on or blinking, the green LED is off.

[26] POST – Power-On Self-Test

[27] Off when the system is powered off or in a sleep state

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:

- MWGUI[28]
- 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 appliance. Users have to authenticate to the module with a valid certificate before they can access any of the user services.

2.4.3 Services

Services provided to authenticated operators are provided in Table 6 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

Table 6 – McAfee Web Gateway Services

Service	Description	Operator		Approved Algorithms Accessed	Type of Access
		CO	User		
Perform initial configuration	Configure the primary network interface, IP[29] address, host name, and DNS[30] server	X		N/A	None

[28] MWGUI – McAfee Web Gateway Graphical User Interface
[29] IP – Internet Protocol
[30] DNS – Domain Name System

Service	Description	Operator		Approved Algorithms Accessed	Type of Access
		CO	User		
CO Login	Crypto-Officer login	X		AES, Triple-DES, RSA, SHA, HMAC, SP 800-90A DRBG	DH[31] Establishment Public Key – RX; DH Establishment Private Key – RX; RSA[32] 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[33] Private Key – RW; Root CA Public Key – RW; RADIUS Shared Secret – WX; LDAP Account Password – WX; NTLM Account Password – WX
Import a license*	Import a license	X		N/A	None
Modify configuration settings*	Modify 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[34] Authentication Key – WX; SNMP v3 Password – WX; NTLM 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 Account Password – WX; SNMP v3 Password – WX;
Backup appliance configuration*	Store the 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

[31] DH – Diffie Hellman
[32] RSA – Rivest, Shamir, and Adleman
[33] CA – Certificate Authority
[34] WCCP – Web Cache Communication Protocol

Service	Description	Operator		Approved Algorithms Accessed	Type of Access
		CO	User		
Restore appliance configuration*	Restore the 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 Keys, WCCP Key – WX
Monitor system functions*	Monitor how the 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[35] *	Shutdown or restart the appliance; 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.					

[35] 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 Public Key – RWX; DH Establishment Private Key – 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 6, the modules provide non-security relavent services. The non-security relevant 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[36]
- 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 7 for the authentication methods used by operators to authenticate the module and assume an authorized role.

[36] SWPS – Secure Web Protection Service

Table 7 – 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 module firmware. 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

The McAfee Web Gateway 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 1 physical security requirements.

2.6 Operational Environment

The operational environment of the the McAfee Web Gateway consists of the module's firmware (v7.3.2.3.4) executing on a non-modifiable version of McAfee's Linux Operating System (MLOS v2.2.3). The OS has a limited operational environment, and only the module's custom-written image can be run on the system.

2.7 Cryptographic Key Management

The module's cryptographic functionality is provided by a firmware library (McAfee Linux OpenSSL library) that offers secure networking protocols and cryptographic functionalities. This firmware library is integrated as part of the underlying operating system. Security functions offered by the module map to the certificates listed in Table 8.

Table 8 – Algorithm Certificate Numbers for Cryptographic Libraries

Approved Security Function	Certificate Number
Symmetric Key Algorithm	
AES[37]: 128-, 192-, 256-bit in CBC[38] mode	3116
Triple-DES[39] : 168-bit in CBC mode	1787
Secure Hashing Algorithm (SHA)	
SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	2572
Message Authentication Code (MAC) Function	
HMAC[40] using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	1953
Deterministic Random Bit Generator (DRBG)	
SP800-90A CTR_DRBG	627
Asymmetric Key Algorithm	
RSA[41] Key Pair Generation (FIPS 186-4) with 2048-bit keys	1587
RSA PKCS[42] #1 v1.5 Signature Generation (FIPS 186-4) with 2048-bit keys	1587
RSA PKCS #1 v1.5 Signature Verification (FIPS 186-2) with 1024-, 1536-, 2048-, 3072-, 4096-bit keys	1587
Digital Signature Algorithm (DSA) Signature Verification: 1024-bit keys	900

Additional information concerning SHA-1 and 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.

[37] AES – Advanced Encryption Standard
[38] CBC – Cipher-Block Chaining
[39] DES – Data Encryption Standard
[40] HMAC – (Keyed-) Hash Message Authentication Code
[41] RSA – Rivest Shamir, Adleman
[42] PKCS – Public Key Cryptography Standards

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 the CMVP. There certificate numbers are provided in Table 9. The complete protocol implementations have not been reviewed or tested by the CAVP[43] and CMVP.

Table 9 – Network Protocol Component Validation

Algorithm	CVL[44] Certificate Number
TLS 1.0/1.1 and TLS 1.2 KDF[45] using SHA 256 and SHA 384	378
SNMP KDF using SHA-1	378

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 8. Its use is allowed per FIPS 140-2 Implementation Guidance 7.11.

[43] CAVP – Cryptographic Algorithm Validation Program
[44] CVL – Component Validation List
[45] KDF – Key Derivation Function

The module supports the CSPs listed below in Table 10.

Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Crypto-Officer Password	Password	Set via MWGUIor 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[46] 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 appliance is re-imaged	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

[46] 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 following FIPS 186-4	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 internally	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[47] control packets

[47] UDP – User Datagram Protocol

2.8 EMI/EMC

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

2.9 Self-Tests

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

2.9.1 Power-Up Self-Tests

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

- Firmware integrity check using HMAC SHA-256
- 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 fails, the module enters into a critical error state where all cryptographic operations and output of any data is prohibited.

The module indicates that it is in an error state when the status output indicating an error is provided via the management port. An example output is as follows:

- Firmware integrity test failure message: "FIPS Self Test failed: RPM verify failed <description of what failed > System halted"
- Cryptographic algorithm test failure message: "FIPS Self Test failed: <Date> : <Process name> (<process pid>) : <openssl reason string> System halted"

Operators can reboot or power-cycle the module, to try to clear the error and resume normal operation.

2.9.2 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 (sign and verify operations)

If any of the tests listed above fails, the module enters into the critical error state where all cryptographic operations and output of any data is prohibited. Operators can reboot or power-cycle the module, to try to clear the error and resume normal operation.

2.10 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.

3 Secure Operation

The McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances meet Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module operation.

3.1 Initial Setup

The following sections provide the necessary step-by-step instructions necessary to configure the module for operation. McAfee delivers the module via trusted delivery services (FedEx, Expeditors International, and Airgroup Express). For any questions or issues that arise at any point during the installation and configuration of the appliance, contact the McAfee support team at http://www.mcafee.com/us/support.aspx.

3.1.1 Setting FIPS Environment

In order to setup the appliance in its validated configuration, the following steps shall be performed by an authorized individual:

1. Obtain version 7.3.2.3.4 installation image from McAfee's Content & Cloud Security Portal.
2. Write 7.3.2.3.4 image to a USB or CD-ROM media.
   NOTE: From this point onwards, until the appliance is sealed, the appliance must not be left unattended by the operator.
3. Attach keyboard/monitor or serial console to appliance and boot to BIOS. Reset the BIOS setting to their Default settings. Change boot settings to add USB or CD to top of boot order.
4. Reboot with media inserted.
5. Select the FIPS 140-2 Level 1 installation mode and serial or keyboard/video as installation operator interface.
6. Wait for disk reformat, install, and reboot.
7. Follow the procedures included in the module's Product Guide to complete installation using the installation wizard.
8. Follow the instructions in Section 3.2 to ensure that the appliance is completely configured for operation. Change the BIOS boot to be hard drive only and add an administrator password to enter the BIOS.
9. Install the front bezel.

The appliance is now considered to be in its validated configuration. This installation procedure disables logon to the appliance using SSH[48] or from a direct-connected console and implements other features required for FIPS compliance.

Once the module is in its validated configuration, the following needs to be done to maintain compliance:

1. The module shall only boot from the hard drive.
2. The Intel Remote Management Console on the module is disabled by default and shall remain so.
3. The log file encryption and/or anonymization feature shall remain turned off.

3.2 Crypto-Officer Guidance

The Crypto-Officer is responsible for initializing, performing security-relevant configuration, and monitoring the module. The Crypto-Officer is required to set a BIOS password to prevent unauthorized individuals from changing the module's settings. 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.

[48] SSH – Secure Shell

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 power cycling the module.

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.

For details regarding the management of the modules, 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 reimaging the 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 11 in this section describes the acronyms used throughout the document.

Table 11 – Acronyms

Acronym	Definition
AC	Alternating Current
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
CVL	Component Validation List
DB-9	D-subminiature 9-pin connector
DES	Digital Encryption Standard
DNS	Domain Name System
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ID	Identification
I/O	Input/Output
IP	Internet Protocol
KAT	Known Answer Test

Acronym	Definition
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MD	Message Digest
MLOS	McAfee Linux Operating System
MWGUI	McAfee Web Gateway Graphical User Interface
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTLM	Microsoft Windows NT LAN Manager
NMI	Non-Maskable interrupt
OS	Operating System
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PKCS	Public Key Cryptography Standard
POST	Power-On Self-Test
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Inexpensive Disks
RC	Rivest Cipher
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
USB	Universal Serial Bus
USM	User-based Security Model
UTF	Unicode Transformation Format
UUID	Universally Unique Identifier
VGA	Video Graphics Array
WCCP	Web Cache Communication Protocol

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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