Certification Report

EAL 2+ Evaluation of Web Gateway v7.0.1.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-89-CR
Version: 1.0
Date: 17 December 2010
Pagination: i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Domus ITSL located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 17 December 2010, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- McAfee
- ePolicy Orchestrator

TABLE OF CONTENTS

Executive Summary

McAfee Web Gateway v7.0.1.1 (hereafter referred to as MWG), from McAfee Inc. is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

MWG software is typically deployed as a web gateway between the internet and the enterprise. MWG provides filters which adapt traffic for various internet protocols including HTTP, HTTPS, and FTP. When it is installed in an FTP system, every transaction is piped through it for filtering and malware scanning on the content. As such, MWG functions as a web gateway to examine and adapt network traffic through a variety of filters to meet the needs of an enterprise. MWG protects against threats such as malware hidden in blended content.

Domus ITSL is the CCEF that conducted the evaluation. This evaluation was completed on 29 November 2010 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for MWG, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that MWG evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented, evaluation is McAfee Web Gateway v7.0.1.1 (hereafter referred to as MWG), from McAfee Inc.

2 TOE Description

MWG software is typically deployed as a web gateway between the internet and the enterprise. MWG provides filters which adapt traffic for various internet protocols including HTTP, HTTPS, and FTP. When it is installed in an FTP system, every transaction is piped through it for filtering and malware scanning on the content. As such, MWG functions as a web gateway to examine and adapt network traffic through a variety of filters to meet the needs of an enterprise. MWG protects against threats such as malware hidden in blended content.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for MWG is identified in Section 2.5 of the Security Target (ST).

MWG uses OpenSSL FIPS Object Module Version 1.1.2 (FIPS 140-2 certificate 918) for HTTPS encryption and decryption as detailed below:

Cryptographic Module	**Certificate #**
OpenSSL FIPS Object Module Version 1.1.2	*918*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in MWG:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	613
Advanced Encryption Standard (AES)	FIPS 197	668
Rivest Shamir Adleman (RSA)	FIPS 186-2	310
Secure Hash Algorithm (SHA-1)	FIPS 180-2	701
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	352

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: McAfee® Web Gateway Version 7.0.1.1 EAL2+ ALC_FLR.2 Security Target
Version: Draft J
Date: 10 September 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3.*

MWG is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures

6 Security Policy

MWG implements an information flow control policy to control information allowed to be forwarded by the system; details of this security policy can be found in Section 5 of the ST.

In addition, MWG implements policies pertaining to security audit, user data protection, identification and authentication, protection of security functions and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of MWG should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE and local administration platform do not host public data.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- Human users who are not authorized administrators cannot directly or remotely access the local administration platform.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE and local administration platform are physically secure.

- Information cannot flow between the internal and external networks unless it passes through the TOE.
- The communication path between the TOE and the local administration workstation (browser) is physically protected.
- The Windows OS running on the local administration platform will provide necessary computing services, but will not tamper with browser communications with the TOE.

7.3 Clarification of Scope

The MWG scope of evaluation includes URL filtering, Anti-Malware, HTTPS scanning and Certificate verification.

MWG provides the following functionality that is specifically excluded from the scope of this evaluation:

- Instant Message Protocol;
- Remote administration from connected networks;
- Cluster Management;
- Multiple Authentication Mechanisms;
- High availability;
- ICAP;
- Transparent router and transparent bridge modes;
- Use of multiple administrator roles;
- Use of ePolicy Orchestrator; and
- Kerberos administration.

8 Architectural Information

The TOE is comprised of the following logical components:

- Proxy Subsystem;
- Filter Core Subsystem;
- GUI Manager Subsystem; and
- Services Subsystem.

Web traffic (HTTP, HTTPS, and FTP) flows through the TOE from the Proxy Subsystem to the Filter Core Subsystem and then back to Proxy Subsystem. The GUI Manager Subsystem is used to configure and monitor the TOE. The Services Subsystem provides the necessary tools for the other subsystems to perform their functions.

Further details about the system architecture are proprietary to the developer, and are not provided in this report.

9 Evaluated Configuration

The evaluated configuration for the MWG comprises:

- McAfee Web Gateway version 7.0.1.1 software.

The TOE software version executes properly across the entire family of MWG appliance models (not part of the TOE): WW500, WW1100, WW1900, WW2900, WG5000 and WG5500. The software also executes properly in a virtual environment under VMware ESX, ESXi or VMware Workstation (version 5.5 or later).

Guidance on establishing the evaluated configuration is provided in the MWG 7.0.1.1 Common Criteria Evaluated Configuration Guide published by McAfee.

10 Documentation

The McAfee documents provided to the consumer are as follows:

- MWG 7.0.1.1 Common Criteria Evaluated Configuration Guide, Ref 86-0948035-D
- MWG 7.0.1.1 Common Criteria Evaluated Configuration Guide,Ref 700-2863A00
- MWG 7.0.1 Product Guide, Ref 700-2574A00

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of MWG, including the following areas:

Configuration management: An analysis of the MWG development environment and associated documentation was performed. The evaluator found that the MWG configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the MWG during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the MWG functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the MWG user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to

securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by McAfee for the MWG. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators examined the developer's vulnerability analysis for the MWG and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. The evaluators conducted an independent review of public domain vulnerability databases, relevant standards, and evaluation deliverables to provide assurance that all potential vulnerabilities have been considered. Additionally, the evaluators conducted some penetration testing to validate several of the vendor's claims for non-exploitability.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of Domus ITSL test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
b. Authentication: To confirm correct operation of authentication policies such as inactivity timer, password complexity and authentication failure;
c. Access Control: To confirm correct operation of the configuration and enforcement of role based access control policies;
d. Security Audit: To confirm correct operation of the audit function; and
e. TOE Management: To confirm ability to configure security parameters via the TOE interface.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted.

The penetration tests focused on:

a. Port Scanning: The objective of this test goal is to determine if MWG opens any ports that could be exploited from the network;
b. DOS Attack: The objective of this test goal is to determine if MWG is vulnerable to a DOS (Denial of Service) attack causing the network controller to reboot;
c. Multi-Scan Actions: The objective of this test goal is to determine if MWG can perform multiple types of scanning and verify that the different scans do not interfere with each other; and
d. Session Fixation: The objective of this test goal is to determine if MWG is vulnerable to session fixation attacks.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

12.4 Conduct of Testing

MWG was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at Domus ITSL. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that MWG behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The evaluator recommends that customers follow the MWG 7.0.1.1 Common Criteria Evaluated Configuration Guide to deploy MWG in its evaluated configuration.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DES	Data Encryption Standard
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash-based Message Encryption Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICAP	Internet Content Adaptation Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MWG	McAfee Web Gateway
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada

Acronym/Abbreviation/ Initialization	Description
RSA	Rivet, Shamir, and Aldeman
SHA	Secure Hash Algoritm
ST	Security Target
TOE	Target of Evaluation
URL	Uniform Resource Locator

16 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.
b. Common Criteria for Information Technology Security Evaluation, Version 2.3., August 2005
c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3., August 2005
d. McAfee® Web Gateway Version 7.0.1.1 EAL2+ ALC_FLR.2 Security Target , Rev J, 10 September 2010
e. McAfee Web Gateway EAL2+ ETR, v1.0, 29 November 2010