Certification Report

EAL 2+ Evaluation of McAfee® Web Gateway Version 7.2.0.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-215-CR
Version:	1.0
Date:	20 November 2012
Pagination:	i to iii, 1 to 10

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 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation*, *Version 3.1 Revision 4*. 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 EWA-Canada located in Ottawa, Ontario.

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 20 November, 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® is a registered trademark of McAfee, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

McAfee® Web Gateway Version 7.2.0.1 (hereafter referred to as MWG), from McAfee Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

MWG software 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 inbound threats such as malware hidden in blended content, and it protects organizations from outbound threats such as the potential loss of confidential information that can leak out on web protocols.

It 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 a system, every transaction is piped through it for filtering and malware scanning on the content.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 5 October 2012 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) to which it is asserted that the product satisfies its 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 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting.

[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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is McAfee® Web Gateway Version 7.2.0.1 (hereafter referred to as MWG), from McAfee Inc.

2 TOE Description

MWG software 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 inbound threats such as malware hidden in blended content, and it protects organizations from outbound threats such as the potential loss of confidential information that can leak out on web protocols.

It 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 a system, every transaction is piped through it for filtering and malware scanning on the content.

A detailed description of the MWG architecture is found in Section 2 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for MWG is identified in Section 2 of the Security Target.

4 Security Target

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

Title: McAfee® Web Gateway Version 7.2.0.1 EAL 2 + ALC_FLR.2 Security Target v1.0
Version: 1.0
Date: 5 October 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

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

6 Security Policy

MWG implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section of the ST.

In addition, MWG implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 6 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 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 management platform.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE and 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 management browser is physically or cryptographically protected;
- The operating system running on the management platform will provide necessary computing services, but will not tamper with browser communications with the TOE.

7.3 Clarification of Scope

MWG offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. MWG is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for MWG comprises:

1. The McAfee® Web Gateway Version 7.2.0.1 running on one of the following;
    a. WW500, WW1100, WW1900, WW2900, WG5000, WG5500, WG4000B, WG4500B, WG5000B, or WG5500B appliance;
    b. HP Proliant G6 Blade Server; or
    c. virtual environment under VMware vSphere 4.1.
2. A generic computing platform running Java Runtime Environment (1.6), and a browser (Microsoft Internet Explorer 7.0)

The publication entitled McAfee Web Gateway Version 7.2.0.1 Common Criteria Evaluated Configuration Guide, 20 June 2012 describes the procedures necessary to install and operate MWG in its evaluated configuration.

9 Documentation

The McAfee Inc. documents provided to the consumer are as follows:

a. McAfee Web Gateway Version 7.2.0.1 Common Criteria Evaluated Configuration Guide, 20 June 2012;

b. McAfee Web Gateway Version 7.2 Product Guide, 7.2, 2012;

c. McAfee Web Gateway Version 7.2 Quick Start Guide, 7.2, 2012; and

d. McAfee Web Gateway Version 7.2 Release Notes, 7.2, 2012.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the MWG functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the MWG security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the MWG preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the MWG configuration management system and associated documentation was performed. The evaluators found that the MWG configuration items were clearly marked. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of MWG during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer 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 conducted an independent vulnerability analysis of MWG. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify MWG potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to MWG in its operational environment.

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

11 ITS Product Testing

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

11.1 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.

11.2 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.

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 EWA-Canada 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. Creation of new permission sets: The objective of this test goal is to confirm that new permission sets can be created and enforced;

c. TOE Access: The objective of this test goal is to test the various methods of access the TOE and that user authentication is enforced on each. It also covers testing for concurrent users;

[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.

d. Unintended reboot: The objective of this test goal is to confirm the TOE's response to an unintended reboot/improper shutdown; and

e. Audit overflow: The objective of this test goal is to confirm how the TOE reacts when the maximum size of the audit file is reached.

11.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities; and

b. Leakage Verification. In this test case the TOE is monitored for information leakage during start-up and shutdown.

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

11.4 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 EWA-Canada. 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.

11.5 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.

12 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.

13 Evaluator Comments, Observations and Recommendations

The evaluator recommends that the user read the ST and all supplemental documentation to make sure that all necessary steps are taken to configure the device for operation in its intended environment; critically, the TOE must be installed in "FIPS mode" prior to any other configuration options can be considered. The evaluator strongly recommends that potential administrators engage in professional training to fully understand the multitude of configuration options; careless configuration could lead to security threats such as unexpected privileged account gain.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. McAfee® Web Gateway Version 7.2.0.1 EAL 2 + ALC_FLR.2 Security Target v1.0, 1.0, 5 October 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee, Inc. McAfee® Web Gateway Version 7.2.0.1, v1.0, 5 October 2012.