Certification Report

NDPP v1.1 conformant evaluation of McAfee® Email Gateway (MEG) software v7.0.1, running on appliance models 4000-B, 4500-B, 5000(B, C & C-2U), 5500(B & C), and the Content Security Blade Server

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2012

Document number: 383-4-198-CR
Version: 1.0
Date: 7 December 2012
Pagination: i to iii, 1 to 11

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.

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 7 December 2012, 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® Email Gateway (MEG) software v7.0.1, running on appliance models 4000-B, 4500-B, 5000(B, C & C-2U), 5500(B & C), and the Content Security Blade Server (hereafter referred to as MEG v7.0.1), from McAfee, Inc., is the Target of Evaluation. The MEG v7.0.1 is conformant with the *Protection Profile for Network Devices version 1.1, 8 June 2012.*

MEG v7.0.1 is an e-mail gateway. It is a security appliance that utilizes hardware and software in an integrated appliance to scan traffic between the WAN (Internet) and an internal (protected) network. Through a series of security scanning, detailed content filtering options, alerts and configured actions, the TOE protects user and company IT resources from a variety of email threats. Threats and resource liabilities such as Viruses, Potentially Unwanted Programs (including Spyware), Spam and Phishing attempts are identified and systematically blocked from protected IT resources.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 16 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 MEG v7.0.1, 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 procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the MEG v7.0.1 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

McAfee® Email Gateway (MEG) software v7.0.1, running on appliance models 4000-B, 4500-B, 5000(B, C & C-2U), 5500(B & C), and the Content Security Blade Server (hereafter referred to as MEG v7.0.1), from McAfee, Inc., is the Target of Evaluation. The MEG v7.0.1 is conformant with the *Protection Profile for Network Devices version 1.1, 8 June 2012.*

2 TOE Description

The MEG v7.0.1 is an e-mail gateway. It is a security appliance that utilizes hardware and software in an integrated appliance to scan traffic between the WAN (Internet) and an internal (protected) network. Through a series of security scanning, alert and configured actions and detailed content filtering options, the TOE protects user and company IT resources from a variety of email threats. Threats and resource liabilities such as Viruses, Potentially Unwanted Programs (including Spyware), Spam and Phishing attempts are identified and systematically blocked from protected IT resources.

A detailed description of the MEG v7.0.1 architecture is found in Section 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for MEG v7.0.1 is identified in Section 1.8 of the ST.

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
McAfee Email Gateway, version 7.0.1	*Pending*[2]

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in MEG v7.0.1:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1299, 1429, 1341
Advanced Encryption Standard (AES)	FIPS 197	2013, 2281, 2106
Rivest Shamir Adleman (RSA)	FIPS 186-2	1042, 1172, 1080
Secure Hash Algorithm (SHA-1)	FIPS 180-2	1763, 1963, 1829
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1218, 1280
Digital Signature Algorithm (DSA)	FIPS 186-2	639, 711, 656
Random Number Generation (RNG)	ANSI x9.31 FIPS 186-2	1055,1134, 1081

4 Security Target

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

Title: McAfee® Email Gateway Version 7.0.1 EAL 2 + ALC_FLR.2 Security Target
Version: 2.0
Date: 16 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.*

MEG v7.0.1 is:

a. Conformant to the Protection Profile for Network Devices, v1.1, June 8, 2012.

b. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

- FDP_CMM_EXT.1 - Scan operation
- FDP_CMM_EXT.2 - Scan actions
- FAU_STG_EXT.1 - External audit trail storage
- FAU_STG_EXT.3 - Action in case of loss of audit server connectivity
- FCS_CKM_EXT.4 Cryptographic key zeroization
- FCS_RBG_EXT.1 Cryptographic operation: random bit generation
- FCS_HTTPS_EXT.1 - HTTPS
- FCS_SSH_EXT.1 - SSH

- FCS_TLS_EXT.1 - TLS
- FIA_PMG_EXT.1 - Password management
- FIA_UIA_EXT.1 - User identification and authentication
- FIA_UAU_EXT.2 - Password-based authentication mechanism
- FPT_SKP.1 - Protection of TSF data
- FPT_APW_EXT.1 - Protection of administrator passwords
- FPT_TUD_EXT.1 - Trusted update
- FPT_TST_EXT.1 - TSF testing
- FTA_SSL_EXT.1 - TSF-initiated session locking

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

d. *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

MEG v7.0.1 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 6 of the ST.

In addition, MEG v7.0.1 implements policies pertaining to Anti-Virus & Anti-Spam, Compliance, Quarantine Management, Secure Web Mail, Security Management, and Audit. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of MEG v7.0.1 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:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE;

- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner;

- Information cannot flow between external and internal networks located in different enclaves without passing through the TOE;

- Administrators will receive and install update signature files from the Anti-Virus Vendor and distribute the .dat and associated scanning engine updates to the TOE; and

- The administrator management computer used for remote security management purposes is free from malware or other malicious software.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

7.3 Clarification of Scope

MEG v7.0.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. The MEG v7.0.1 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 MEG v7.0.1 comprises:

The McAfee® Email Gateway (MEG) software v7.0.1 running on one of the following appliances;

- 4000-B;

- 4500-B;

- 5000-B;

- 5000-C;

- 5000-C-2U;

- 5500-B;

- 5500-C; or

- HP C7000 or C3000 Content Security Blade Server with the BL460 blade.

The workstation accessing the TOE via the GUI requires Microsoft Internet Explorer 7.0, 8.0 or 9.0, or Firefox 3.5, 3.6 or 4.0

The publication entitled Common Criteria Evaluated Configuration Guide McAfee® Email Gateway 7.0.1 Appliances, Revision B describes the procedures necessary to install and operate MEG v7.0.1 in its evaluated configuration.

9 Documentation

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

a. Common Criteria Evaluated Configuration Guide McAfee® Email Gateway 7.0.1 Appliances, Revision B;

b. Quick Start Guide for McAfee Email Gateway Appliance Revision A;

c. McAfee Email Gateway Appliances Installation Guide Revision A;

d. Quick Start Guide McAfee Content Security Blade Server Revision A;

e. McAfee Content Security Blade Server Installation Guide Revision A;

f. Administrators guide McAfee Email Gateway 7.0.0 Appliances Revision A ; and

g. Release Notes for McAfee Email Gateway Appliance7.0.1 Release date: November 22, 2011

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of MEG v7.0.1, including the following areas:

Development: The evaluators analyzed the MEG v7.0.1 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 MEG v7.0.1 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 MEG v7.0.1 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 MEG v7.0.1 configuration management system and associated documentation was performed. The evaluators found that the MEG v7.0.1

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 MEG v7.0.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by McAfee® Inc. for MEG v7.0.1. 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 MEG v7.0.1. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify MEG v7.0.1 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to MEG v7.0.1 in its operational environment.

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

11 ITS Product Testing

Testing 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[3].

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.

[3] 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 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; and

b. Protection Profile required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the protection profile to which the TOE is claiming conformance.

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. Protection Profile required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance;

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

c. 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

MEG v7.0.1 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 MEG v7.0.1 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an NDPP v1.1 conformance claim, to 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 potential users of the TOE should also follow all the instructions and recommendations provided in the Guidance Documentation during installation and configuration of the TOE. Additionally it is noted that in order to install the TOE, correct placement within the network, for the configuration you implement, is important. It is recommended that the administrator consult with their IT architect, and the Guidance Documentation, to ensure proper support for the appliance in the environment.

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
GUI	Graphical User Interface
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, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, July 2009.

d. Protection Profile for Network Devices, v1.1, June 8, 2012.

e. McAfee® Email Gateway Version 7.0.1 EAL 2 + ALC_FLR.2 Security Target, 2.0, 16 October 2012.

f. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee, Inc. McAfee® Email Gateway Appliance Version 7.0.1 Version 1.2, 16 October 2012.