Certification Report

EAL 2+ Evaluation of McAfee Email and Web Security Appliance Version 5.5 Patch 2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-143-CR
Version:	1.0
Date:	17 December 2010
Pagination:	i to iii, 1 to 12

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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 IT Security Laboratory 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 is a trademark of McAfee, Inc. in the United States and/or other counties.

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

TABLE OF CONTENTS

Disclaimer i

Foreword ii

Executive Summary 1

1 Identification of Target of Evaluation 3

2 TOE Description 3

3 Evaluated Security Functionality 3

4 Security Target 4

5 Common Criteria Conformance 4

6 Security Policy 4

7 Assumptions and Clarification of Scope 5

7.1 SECURE USAGE ASSUMPTIONS 5
7.2 ENVIRONMENTAL ASSUMPTIONS 5
7.3 CLARIFICATION OF SCOPE 5

8 Architectural Information 5

9 Evaluated Configuration 6

10 Documentation 7

11 Evaluation Analysis Activities 7

12 ITS Product Testing 8

12.1 ASSESSMENT OF DEVELOPER TESTS 9
12.2 INDEPENDENT FUNCTIONAL TESTING 9
12.3 INDEPENDENT PENETRATION TESTING 10
12.4 CONDUCT OF TESTING 10
12.5 TESTING RESULTS 10

13 Results of the Evaluation 10

14 Evaluator Comments, Observations and Recommendations 11

15 Acronyms, Abbreviations and Initializations 11

16 References 11

Executive Summary

McAfee Email and Web Security Appliance Version 5.5 Patch 2 (hereafter referred to as McAfee EWS Appliance), from McAfee, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation

McAfee EWS Appliance is a scalable hardware/software appliance that provides a comprehensive security solution for internet and email services. Through a series of security scanning, alert and configured actions, and detailed content filtering options, the McAfee EWS Appliance protects user and company IT resources from a variety of internet and 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. In addition, content filtering allows administrators to assure that inappropriate content or bandwidth usage is actively thwarted. McAfee EWS Appliance also supports auditing, identification and authentication of administrators, and security management tools.

Various hardware scalability options are available to tailor the software solution to throughput requirements based on the size of the enterprise and number of users. For small to medium sized businesses up to 1000 users, the McAfee EWS Appliance solution is implemented as the email and web security appliance. This consolidated solution includes internet and email protection in a single appliance. For larger businesses, the McAfee EWS Appliance functionality is deployed as the web security appliance offering internet security features and the email security appliance providing email protection features. In this case the requirements of this ST are met by the web and email appliances operating together, rather than by a single appliance. The McAfee EWS Appliance utilizes the same software suite regardless of hardware platform selected, although three different build images are available for the respective appliance functions.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 13 October 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 McAfee EWS Appliance, 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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 –Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that McAfee EWS Appliance 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 Email and Web Security Appliance Version 5.5 Patch 2 (hereafter referred to as McAfee EWS Appliance), from McAfee, Inc..

2 TOE Description

McAfee EWS Appliance is a scalable hardware/software appliance that provides a comprehensive security solution for internet and email services. Through a series of security scanning, alert and configured actions, and detailed content filtering options, the McAfee EWS Appliance protects user and company IT resources from a variety of internet and 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. In addition, content filtering allows administrators to assure that inappropriate content or bandwidth usage is actively thwarted. McAfee EWS Appliance also supports auditing, identification and authentication of administrators, and security management tools.

Various hardware scalability options are available to tailor the software solution to throughput requirements based on the size of the enterprise and number of users. For small to medium sized businesses up to 1000 users, the McAfee EWS Appliance solution is implemented as the email and web security appliance. This consolidated solution includes internet and email protection in a single appliance. For larger businesses, the McAfee EWS Appliance functionality is deployed as the web security appliance offering internet security features and the email security appliance providing email protection features. In this case the requirements of this ST are met by the web and email appliances operating together, rather than by a single appliance. The McAfee EWS Appliance utilizes the same software suite regardless of hardware platform selected, although three different build images are available for the respective appliance functions.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for McAfee EWS Appliance is identified in Section 5 of the Security Target (ST).

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in McAfee EWS Appliance:

Cryptographic Algorithm	Standard	Certificate #
SHA1	FIPS 180-3	SHS679

4 Security Target

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

Title: McAfee Email and Web Security Appliance Version 5.5 Patch 2
Version: DRAFT 0.12
Date: 22 July 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

McAfee EWS Appliance is:

a. *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_MAM.1, Malware Monitoring, Scan Operation;
   - FDP_MAM.2, Malware Monitoring, Scan Actions; and
   - FDP_MAM.3, Malware Monitoring, Potential Violation Analysis.

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 3 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

McAfee EWS Appliance implements an anti-virus security policy to provide protection from viruses and malicious programs and take a specific action upon identification of a virus/malware/spyware, as well as a content scanning and filtering policy to identify or restrict access to intercepted traffic.

In addition, McAfee EWS Appliance implements policies pertaining to security audit, identification and authentication, verification of downloaded threat signature files, 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 McAfee EWS Appliance 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 Administrators of the TOE are assumed to be non-hostile, competent, trustworthy and to follow the guidelines supplied in guidance documentation.
- The McAfee EWS Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.
- 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.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
- The administrator management computer used for remote security management purposes is to be free of malware or other malicious software.

7.3 Clarification of Scope

The following items are specifically excluded from the TOE:

- McAfee E-Policy Orchestrator (software)
- The use of LDAP or Kerberos authentication servers
- Scanning of TLS traffic
- Remote Access Card option for the 3300/3400 appliances (Enterprise)
- Administration from a remote location using the Remote Access Card
- Protection of the link to the management computer using HTTPS
- Export of log records to an external server

8 Architectural Information

The McAfee EWS Appliance architecture is divided into the following modules:

- Anti-Virus Module;
- PUP Module (including Spyware);
- Anti-Phishing Module;
- Anti-Spam Module;
- URL Filtering Module;

- Content Scan Module;
- Quarantine Management Module;
- ICAP support Module;
- HTTP Scan Module; and
- EWS Security Management Operating System.

The software of the McAfee EWS Appliance is identical among all evaluated configurations of the appliance. The service or functionality that is enabled is dependent upon the hardware platform deployed. In the case of the Email and Web Security appliance all the software modules execute on that single hardware appliance. In the case of the Email Security Appliance and Web Security Appliance, those modules that correspond to the selected hardware platform are enabled based on that platform (either email or web).

The McAfee EWS appliance allows creation of virtual hosts. Using virtual hosts, a single appliance can appear to behave like several appliances. Each virtual appliance can manage traffic within specified pools of IP addresses, enabling the appliance to provide scanning services to traffic from many sources or customers.

The McAfee EWS appliance also allows grouping of appliances into clusters. A cluster is a group of appliances that shares both its configuration and balances the network traffic. The cluster can contain:

- One cluster master. The master both synchronizes the configuration and balances the load of network traffic to the other cluster members.

and at least one of the following:

- One cluster failover. If the cluster master fails, the cluster failover will seamlessly take over the work of the cluster master.
- One or more cluster scanners. They scan traffic according to the policies synchronized from the master.

Note that the master and the failover can also scan traffic.

Further details about the system architecture may be found in Section 1.6 of the ST.

9 Evaluated Configuration

The evaluated configuration for McAfee EWS Appliance comprises both hardware models and software.

The TOE is the McAfee Email and Web Security software v5.5 Patch 2 running on appliance models 3000, 3100, 3200, 3300, 3400, the Content Security Blade Server, and VMware Server. The software includes the EWS operating system.

The following Model identifiers are included in the evaluated configuration:

- Email and Web Security Appliance for the 3000 platform: SKU = EWS-3000-00A;
- Email and Web Security Appliance for the 3100 platform: SKU = EWS-3100-00A;
- Email and Web Security Appliance for the 3200 platform: SKU = EWS-3200-00A;
- Email and Web Security Appliance for the 3300 platform: SKU = EWS-3300-00A;
- Email Security Appliance for the 3400 platform: SKU = EWS-3400-SMA; and
- Web Security Appliance for the 3400 platform: SKU = EWS-3400-SWA.

- Blade enclosure SKUs: MCS-CH1P-M72 (M7 single phase power);
  MCS-CHDP-M7C (M7 DC power);
  MCS-CH3I-M72 (M7 3 phase international);
  MCS-CH3P-M72 (M7 DC international); and
  MCS-CH1P-M31 (M3 single phase AC).

- Blade SKUs: Management MCS-MGMT-MXX; and
  Scanning MSC-BLDE-1XX.

- SKU for VMware Not applicable – available as web download only.

For details on the evaluated configuration, refer to Section 1.8 of the ST.

10 Documentation

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

- Quick Start Guide for McAfee Email and Web Security Appliance v5.5;
- McAfee Email and Web Security Appliance 5.5 Installation Guide;
- McAfee Email and Web Security Virtual Appliance 5.5 Installation Guide;
- McAfee Email and Web Security Appliance (VMtrial) 5.5 Installation Guide;
- McAfee Email and Web Security Appliance 5.5 Migration Guide;
- Quick Start Guide for McAfee Content Security Blade Server (M3 chassis);
- Quick Start Guide for McAfee Content Security Blade Server (M7 chassis);
- McAfee Content Security Blade Server 5.5 (M3 chassis) Installation Guide;
- McAfee Content Security Blade Server 5.5 (M7 chassis) Installation Guide;
- McAfee Email and Web Security Appliance 5.5 Product Guide;
- Release Notes for McAfee Email and Web Security Appliance 5.5; and
- McAfee Email and Web Gateway and McAfee ePolicy Orchestrator Integration Guide (out of scope of the TOE).

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee EWS Appliance, including the following areas:

Development: The evaluators analyzed the McAfee EWS Appliance 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 McAfee EWS Appliance 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 McAfee EWS Appliance 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 McAfee EWS Appliance configuration management system and associated documentation was performed. The evaluators found that the McAfee EWS Appliance 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 McAfee EWS Appliance during distribution to the consumer.

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

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.

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 IT Security Laboratory 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. Anti-Virus: The objective of this test goal is to determine the TOE's ability to provide protection from viruses and malicious programs via a scanning engine and to verify that alarms are generated for selected events;
c. Audit: The objective of these tests is to ensure that the audit generation, selectable audit, storage and protection of audit records, audit review, and audit report generation requirements have been met;
d. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized administrators only;
e. Filtering: The objective of these tests is to determine the TOE's ability to identify suspect email messages and/or email attachments and take the specified action;
f. Action and Remediation: The objective of these tests is to verify that the TOE performs the configured action upon intercepted traffic;
g. Cryptographic Operations: The objective of these tests is to verify the verification process used by the TOE for downloaded threat signature files; and
h. Security Management: The objective of this test goal is to determine the correct operation of the management functions provided by the TOE.

[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.

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 the McAfee EWS Appliance opens any ports that could be exploited from the network;
b. Packet Scanning: The objective of this test goal is to determine if the network packets are encrypted when HTTPS is enabled;
c. Session Fixation: The objective of this test goal is to determine if the McAfee EWS Appliance is vulnerable to the session fixation attack;
d. DOS (Denial of Service) Attack: The objective of this test goal is to determine if the McAfee EWS Appliance is vulnerable to a DOS attack causing the network controller to reboot;
e. Multi-Scan Actions: The objective of this test goal is to determine if the McAfee EWS Appliance can perform multiple types of scanning and verify that the different scans do not interfere with each other; and
f. IP Use: The objective of this test goal is to determine if the McAfee EWS Appliance allows the use of the IP of a restricted website when the site has been blocked.

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

12.4 Conduct of Testing

McAfee EWS Appliance 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 IT Security Laboratory. 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 McAfee EWS Appliance 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 found the guidance for the configuration, use, and integration of the McAfee EWS Appliance in its evaluated configuration to be clear. The evaluator recommends that customers follow the provided guidance documentation in order to deploy the McAfee EWS Appliance in its evaluated configuration.

15 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
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EWS	Email and Web Security
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol Secure
HTTPS	HTTP Secure
ICAP	Internet Content Adaptation Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LDAP	Lightweight Directory Access Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
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. CC version e.g. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July, 2009.

c. CEM version e.g. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. McAfee Email and Web Security Appliance Version 5.5 Patch 2, DRAFT 0.12, 22 July 2010

e. McAfee Email and Web Security Appliance Evaluation Technical Report, version 1.0, 13 October 2010