Certification Report

EAL 4+ Evaluation of McAfee Firewall Enterprise v8.2.0 and McAfee Firewall Enterprise Control Center v5.2.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-182-CR
Version: 1.0
Date: 27 January 2012
Pagination: i to iii, 1 to 13

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 EWA-Canada 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 27 January 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 registered trademarks:

- McAfee is a registered trademark of McAfee Inc; and
- UNIX is a registered trademark of The Open Group.

TABLE OF CONTENTS

Executive Summary

The McAfee Firewall Enterprise v8.2.0 and McAfee Firewall Enterprise Control Center v5.2.0 (hereafter referred to as McAfee Firewall Enterprise), from McAfee, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

The McAfee Firewall Enterprise is a software-only TOE which operates with two or more network interfaces to provide a hybrid firewall solution that supports both application-level proxy and packet filtering. The McAfee Firewall software consists of a collection of integrated firewall applications and SecureOS, a secure operating system. Secure OS is an extended version of the FreeBSD UNIX operating system which provides the secured computing environment in which all McAfee Firewall application layer processing is performed. McAfee Firewall also provides VPN capability between separated network enclaves. McAfee Firewall Enterprise establishes encrypted communications with authorized remote users and external IT entities using a FIPS 140-2 validated cryptographic module. Management of the McAfee Firewall may be carried out using either the McAfee Firewall Admin Console or the McAfee Firewall Enterprise Control Center.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 10 January 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 McAfee Firewall Enterprise, 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 4 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.3 – Systematic Flaw Remediation.

McAfee Firewall Enterprise is conformant with the *U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments Version 1.1, July 25, 2007.*

[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 McAfee Firewall Enterprise 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) 4 augmented evaluation is McAfee Firewall Enterprise v8.2.0 and McAfee Firewall Enterprise Control Center v5.2.0 (hereafter referred to as McAfee Firewall Enterprise), from McAfee.

2 TOE Description

McAfee Firewall Enterprise is a software-only TOE which operates with two or more network interfaces to provide a hybrid firewall solution that supports both application-level proxy and packet filtering. The McAfee Firewall software consists of a collection of integrated firewall applications and SecureOS, a secure operating system. Secure OS is an extended version of the FreeBSD UNIX operating system which provides the secured computing environment in which all McAfee Firewall application layer processing is performed. McAfee Firewall also provides VPN capability between separated network enclaves using a FIPS 140-2 validated cryptographic module. Management of the McAfee Firewall may be carried out using either the McAfee Firewall Admin Console or the McAfee Firewall Enterprise Control Center.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for McAfee Firewall Enterprise is identified in Section 5 of the ST.

McAfee Firewall provides VPN capability between separated network enclaves. McAfee Firewall Enterprise establishes encrypted communications with authorized remote users and external IT entities using a FIPS-140-2 validated cryptographic module.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
McAfee Firewall Enterprise 1100F	*Pending* [2]
McAfee Firewall Enterprise 2150F	*Pending*
McAfee Firewall Enterprise 4150F	*Pending*
McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032, S6032	*Pending*
McAfee Firewall Enterprise Control Centre Virtual Appliance	*Pending*

[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.

McAfee Firewall Enterprise Control Centre C1015, C2050, C2000	*Pending*

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

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	765, 766, 1185
Advanced Encryption Standard (AES)	FIPS 197	972, 973, 1833
Rivest Shamir Adleman (RSA)	FIPS 186-2	469, 470
Digital Signature Algorithm (DSA)	FIPS 186-3	338, 339
Secure Hash Algorithm (SHA-1)	FIPS 180-3	941, 942, 1612
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	544, 545, 1086
Pseudo Random Number Generator (PRNG)	ANSI X93.1	549, 550, 964

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in McAfee Firewall Enterprise Control Centre Virtual Appliance:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1209, 1247
Advanced Encryption Standard (AES)	FIPS 197	1862, 1917
Rivest Shamir Adleman (RSA)	FIPS 186-2	943, 985
Digital Signature Algorithm (DSA)	FIPS 186-3	581, 608
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1638, 1683
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1109, 1152
Pseudo Random Number Generator (PRNG)	ANSI X93.1	976, 1008

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in McAfee Firewall Enterprise Control Center:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1184, 1233
Advanced Encryption Standard (AES)	FIPS 197	1813, 1897
Rivest Shamir Adleman (RSA)	FIPS 186-2	920, 972
Digital Signature Algorithm (DSA)	FIPS 186-3	575, 599
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1611, 1666
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1085, 1137
Pseudo Random Number Generator (PRNG)	ANSI X93.1	963, 1009

4 Security Target

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

Title: McAfee Firewall Enterprise v8.2.0 and McAfee Firewall Enterprise Control Center v5.2.0 Security Target
Version: Version 1.1
Date: 10 January 2012

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 Firewall Enterprise is:

a. *Common Criteria Part 2 extended;* with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:
    - FIA_UAU.8(X) – Invocation of authentication mechanisms.
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3;
c. *Common Criteria EAL 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation; and
d. McAfee Firewall Enterprise is conformant with the *U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments Version 1.1, July 25, 2007.*

6 Security Policy

McAfee Firewall Enterprise implements four security policies:

The Unauthenticated Information Flow Policy is based upon the source, destination, and content of network packets (protocol connection attributes) without requiring subject authentication. Based on this policy McAfee Firewall can either discard or pass information;

The Authenticated Information Flow Policy is based upon the source, destination, and content of network packets (protocol connection attributes). In order for information to flow subjects must first successfully authenticate to McAfee Firewall. Based on this policy McAfee Firewall can either discard or pass information;

The VPN security policy is based on source and destination identifiers from the network packet. Based on the VPN security policy McAfee Firewall can either pass information without modification, decrypt, or encrypt; and

The Type Enforcement security policy controls access to the McAfee Firewall audit files and the audit database.

In addition, McAfee Firewall Enterprise implements policies pertaining to Security Audit, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Trusted Path/Channels and Cryptographic Support. Further details on these security policies may be found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of McAfee Firewall Enterprise 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:

- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error;
- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE;
- Authorized administrators may access the TOE remotely from the internal and external networks; and
- Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is physically secure;
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low;

- There are no general-purpose computing capabilities (e.g. the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;
- The TOE does not host public data; and
- Information cannot flow among the internal and external networks unless it passes through the TOE.

7.3 Clarification of Scope

McAfee Firewall Enterprise offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. McAfee Firewall Enterprise 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 McAfee Firewall Enterprise comprises:

a. McAfee Firewall Enterprise version 8.2.0 running on McAfee appliances: S1104, S2008, S4016, S6032, 1100F, 2150F, 4150F, and on VMWare ESXi v4.1;
b. McAfee Firewall Enterprise Control Center version 5.2.0 running on McAfee appliances: C1015, C2050, C3000, and on VMWare ESXi v4.1; and
c. McAfee Admin Console version 5.0.5 running on MS Windows 2008 Server, Windows XP Professional, Windows Vista, and Windows 7.

The publications entitled *McAfee Firewall Enterprise Quick Start Guide Version 8.2.X, McAfee Firewall Enterprise Virtual Appliance Installation Guide Version 8.X* and *McAfee Firewall Enterprise Control Center Quick Start Guide Version 5.2.X describe the procedures necessary to install and operate McAfee Firewall Enterprise in its evaluated configuration.*

9 Documentation

The McAfee documents provided to the consumer are as follows:

a. McAfee® Firewall Enterprise Release Notes version 8.2.0, 700-3493A00;

b. McAfee® Firewall Enterprise Control Center Release Notes version 5.2.0, 700-3466A00;

c. McAfee Firewall Enterprise Product Guide Version 8.2.0, 700-3494A00;

d. McAfee Firewall Enterprise Installation USB Drive Version 8.2.X, 700-3510A00;

e. McAfee Firewall Enterprise Quick Start Guide Version 8.2.X, 700-3508A00;

f. McAfee Firewall Enterprise Reference Guide Command line Interface Version 8.2.X, 700-3498A00;

g. McAfee Firewall Enterprise Virtual Appliance Installation Guide Version 8.X, 700-3495A00;

h. McAfee Firewall Enterprise Control Center Product Guide Version 5.2.0, 700-3462A00;

i. McAfee Firewall Enterprise Control Center Quick Start Guide Version 5.2.X, 700-3457A00;

j. McAfee Firewall Enterprise Control Center Virtual Appliance Installation Guide Version 5.2.X, 700-3461A00; and

k. McAfee Firewall Enterprise Common Criteria Evaluated Configuration Guide Version 8.2.0, 700-3512A00.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee Firewall Enterprise, including the following areas:

Development: The evaluators analyzed the McAfee Firewall Enterprise functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the McAfee Firewall Enterprise security architectural description and determined that the initialization process is secure and 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 Firewall Enterprise 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 Firewall Enterprise configuration management system and associated documentation was performed. The evaluators found that the McAfee Firewall Enterprise configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access

control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

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

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the McAfee Firewall Enterprise design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by McAfee for McAfee Firewall Enterprise. 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 Firewall Enterprise. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the McAfee Firewall Enterprise in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 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 and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's

[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.

test documentation and the functional specification, TOE design and security architecture description 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. Initialization: The purpose of this test was to perform the customer install, generation, and startup procedures to install the McAfee Firewall Enterprise and configure it to be consistent with the Developer's guidance documentation;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests; and

c. Independent Testing: The objective of this test goal is to prove or disprove the security claims made by the vendor through positive and negative oriented functional testing. The following independent test cases were executed:

    i. Telnet Server Authentication Failure Processing: This test case verifies that all connection attempts are audited and that a delay occurs after the fourth unsuccessful attempt;

    ii. Console Login Failure Processing: This test case verifies that all connection attempts are audited and that a delay occurs after the fourth unsuccessful attempt;

    iii. Control-D Delay Bypass: This test case verifies that the [Ctrl-D] bypass is handled correctly;

    iv. Time Stamp Logs: This test case validates that various log files contain the correct event time stamps;

    v. Time Stamp on Files: This test case validates that the time stamps on files are consistent with the system time;

    vi. Time Control: This test case validates that only the administrator with full administrator rights can change the date and time;

vii. Configuring Time through the Admin Console: This test case validates that only the administrator with full administrator rights can change the date and time; and

viii. Modify Memory: This test case validates that the memory is protected even when a user has full administrator privileges.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Port Scan: The purpose of this test case is to identify all open ports on the TOE;

b. Monitor for Information Leakage: The purpose of this test is to determine if the TOE is leaking any information that might be useful to an attacker;

c. Communications failure: The purpose of this test is to verify how the TOE behaves under extreme circumstances such as communications failure as a result of a disruption to the connection or power;

d. Session Management – Concurrent Admin Sessions: The purpose of this test is to determine how the TOE responds to concurrent administrator logins; and

e. Tampering – SQL Injections: The purpose of this test is to determine if the TOE prevents SQL injection attacks at login.

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

11.4 Conduct of Testing

McAfee Firewall Enterprise 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, as well as at the McAfee development location. 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 McAfee Firewall Enterprise behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 + level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

14 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 3, July 2009.

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

d. U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments Version 1.1, July 25, 2007.

e. McAfee Firewall Enterprise v8.2.0 and McAfee Firewall Enterprise Control Center v5.2.0 Security Target, Version 1.1, 10 January 2012.

f. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of McAfee, Inc McAfee Firewall Enterprise v8.2.0 and McAfee Firewall Enterprise Control Center v5.2.0, Version 1.2, 10 January 2012.