Certification Report

McAfee Network Security Platform v7.1

(M-series sensors)

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-243-CR
Version: 1.0
Date: 10 September 2013
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 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.

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 19 August 2013, 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.

TABLE OF CONTENTS

Executive Summary

McAfee Network Security Platform v7.1 (M-series sensors) (hereafter referred to as McAfee NSP), from McAfee, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

McAfee NSP is an Intrusion Detection System (IDS) product that is a combination of network appliances and software built for the detection of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks and network misuse.

McAfee NSP is composed of a family of sensor appliances and a NSP Management platform referred to as NSM. The sensor platforms are stand-alone appliances from McAfee Inc. All other components of the product are software only components that run on Windows.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 19 July 2013 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 NSP, 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 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 the McAfee NSP 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 Network Security Platform v7.1 (M-series sensors) (hereafter referred to as McAfee NSP), from McAfee, Inc.

2 TOE Description

McAfee NSP is an Intrusion Detection System (IDS) product that is a combination of network appliances and software built for the detection of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks and network misuse.

McAfee NSP is composed of a family of sensor appliances and a NSP Management platform referred to as NSM. The sensor platforms are stand-alone appliances from McAfee Inc. All other components of the product are software only components that run on Windows.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for McAfee NSP is identified in Section 6 of the ST.

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

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	880, 2468, 2469
Rivest Shamir Adleman (RSA)	FIPS 186-2	425, 830, 1258, 1259
Secure Hash Algorithm (SHA-1)	FIPS 180-2	871, 970, 2082, 2083
Keyed-Hash Message Authentication Code and Secure Hash Algoritm (HMAC-SHA1)	FIPS 198	971, 1512, 1513
Random Number Generator (RNG)	FIPS 186-2, ANSI X-.31	505, 1197, 1198

4 Security Target

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

Title: McAfee Network Security Platform (NSP) Security Target (M-series sensors)
Version: 1.0
Date: 19 July 2013

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 NSP 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:
   - IDS_SDC.1 - System Data Collection;
   - IDS_ANL.1 - Analyser Analysis;
   - IDS_RCT.1 - Analyser React;
   - IDS_RDR.1 - Restricted Data Review;
   - IDS_STG.1 - Guarantee of System Data Availability; and
   - IDS_STG.2 - Prevention of Data Loss.

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

c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2– Flaw reporting procedures.

6 Security Policy

McAfee NSP implements a User Data policy to control how user data within the TOE can be manipulated, as well as a User Role Policy to determine permissions to modify user data; details of these security policies can be found in Section 6 of the ST.

In addition, McAfee NSP implements other policies pertaining to security audit, identification and authentication, security management, Protection of the TSF, System Data Collection, System Data Analysis and System Data Review. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of McAfee NSP 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 will be one or more competent individuals assigned to manage the TOE and the security of the information it contains;
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation; and
- The TOE can only be accessed by authorized users.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT System data it needs to perform its functions;
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors;
- The TOE is appropriately scalable to the IT System the TOE monitors;
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification; and
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

McAfee NSP incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

The evaluated configuration for McAfee NSP comprises one or more of the sensors listed below running the NSP Sensor software version 7.1.15.4, and the Network Security Manager (NSM) version 7.1.15.1.11.

Model Number	**Part Number**	**Revision**
Sensor M-1450	600-1230-04-G	D
Sensor M-1250	600-1231-04-G	D
Sensor M-2750	600-1209-03-G	D
Sensor M-2850	600-1470-03-G	D
Sensor M-2950	600-1429-01-G	D
Sensor M-6050	600-1220-07-G	E
Sensor M-4050	600-1245-06-G	F
Sensor M-3050	600-1246-06-G	F

Sensor M-8000	600-1221-07-G (Primary)	E
	600-1222-07-G (Secondary)	E

The publication entitled Network Security Platform 7.1 Common Criteria Evaluated Configuration Guide EAL 2 + ALC_FLR.2 Revision A describes the procedures necessary to install and operate McAfee NSP in its evaluated configuration.

9 Documentation

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

- Getting started guide Revision B, McAfee Network Security Platform 7.1;
- Installation Guide Revision H, McAfee Network Security Platform 7.1;
- IPS Administration Guide Revision K, McAfee Network Security Platform 7.1;
- Manager Administration Guide Revision K, McAfee Network Security Platform 7.1;
- Custom Attack Definitions Guide Revision D, McAfee Network Security Platform 7.1;
- Network Security Platform 7.1 Device Administration Guide Revision E, McAfee Network Security Platform 7.1;
- Best Practices Guide Revision K, McAfee Network Security Platform 7.1;
- Network Security Platform 7.1 Common Criteria Evaluated Configuration Guide EAL 2 + ALC_FLR.2 Revision A;
- M-6050 Sensor Quick Start Guide Revision A, McAfee Network Security Platform 7.1;
- M-8000 Sensor Quick Start Guide Revision A, McAfee Network Security Platform 7.1;
- M-1250/M1450 Sensor Quick Start Guide Revision A, McAfee Network Security Platform 7.1;
- M-2750 Sensor Quick Start Guide Revision A, McAfee Network Security Platform 7.1;
- M-2850/M-2950 Sensor Quick Start Guide Revision A, McAfee Network Security Platform 7.1;
- M-3050/M-4050 Sensor Quick Start Guide Revision A, McAfee Network Security Platform 7.1;
- M-1250/M-1450 Sensor Product Guide Revision A, McAfee Network Security Platform 7.1;
- M-2750 Sensor Product Guide Revision A, McAfee Network Security Platform 7.1;
- M-2850/M-2950 Sensor Product Guide Revision A, McAfee Network Security Platform 7.1;
- M-3050/M-4050 Sensor Product Guide Revision A, McAfee Network Security Platform 7.1;
- M-6050 Sensor Product Guide Revision A, McAfee Network Security Platform 7.1; and

- M-8000 Sensor Product Guide Revision A, McAfee Network Security Platform 7.1.

10 Evaluation Analysis Activities

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

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

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee NSP. 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 NSP. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify McAfee NSP potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to McAfee NSP 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[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. Logging in with CAC credentials: The objective of this test goal is to confirm that users may log into the TOE using CAC credentials;

c. Bypass CAC credentials; The objective of this test goal is to confirm that users may not access TOE functionality without the appropriate CAC credentials;

d. Internal Data Transfer Protection: The objective of this test goal is to confirm that data transferred between different parts of the TOE are protected as described in the ST.

e. User Role Permissions: The objective of this test goal is to verify that the role permissions are enforced as described in the ST; and

[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.

f. Signature Set Updates: The objective of this test goal is to verify that valid signature sets may be deployed and that invalid ones are rejected and that both events are audited.

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. Port Scan: The objective of this test goal is verify that only those ports that should be open, are;

b. Inactivity Timeout: The objective of this test goal is to verify that the TOE protects itself against an administrative session being left open;

c. Banner Grabbing: The objective of this test goal is to determine if any useful information can be gained from the TOE login screen;

d. Information Leakage Verification: The objective of this test goal is to monitor for data leakage during start-up, shutdown , and login;

e. Concurrent Administrators: The objective of this test goal is to demonstrate that the TOE performs correctly when an administrative user logs on from two locations concurrently; and

f. Nessus and SSL scans: The objective of this test goal is to scan for known and unknown weaknesses relevant to the TOE type.

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

11.4 Conduct of Testing

McAfee NSP was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. Some of the testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada as well as in the Quality Assurance lab at McAfee, Inc. in Santa Clara, California. 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 NSP 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

McAfee NSP is a mature, well documented product. Customers may refer to the most recent version of the documentation for any of the guides listed in the ST. It should be noted that the Common Access Card is the only allowable means of authentication in the evaluated product configuration.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CAVP	Cryptographic Algorithm Validation Program
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DDoS	Distributed Denial of Service
DoS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC-SHA1	Keyed Hash Message Authenticated Code and Secure Hash Algorithm
IDS	Intrusion Detection System
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NSP	Network Security Platform
PALCAN	Program for the Accreditation of Laboratories - Canada
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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 Network Security Platform (NSP) Security Target (M-series sensors), version 1.0, 19 July 2013.

e. Evaluation Technical Report for McAfee Network Security Platform 7.1.15.1 (m-Series sensors) version 1.1, 19 July 2013.