# Certification Report

## McAfee Network Security Platform M-Series and NS-Series Sensors

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**

| | |
|---|---|
| **Document number**: | 383-4-289-CR |
| **Version**: | 1.0 |
| **Date**: | 3 May 2016 |
| **Pagination**: | i to iii, 1 to 9 |

## 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, applies 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, 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, 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) provide 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.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 3 May 2016 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).

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

**TABLE OF CONTENTS**

## Executive Summary

McAfee Network Security Platform M-Series and NS-Series Sensors (hereafter referred to as McAfee NSP Sensors), from Intel Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that McAfee NSP Sensors is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

McAfee NSP Sensors are built for the detection of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks and network misuse.

The NSP Sensor component performs:

- Traffic Capture, which captures packets into a data store for review;
- Load balancing and protocol verification, which makes security decisions such that it can filter packets of no interest;
- Denial of Service detection and response; and
- Signature detection and anomaly detection.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 3 May 2016 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 Sensors, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the McAfee NSP Sensors 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

McAfee Network Security Platform M-Series and NS-Series Sensors (hereafter referred to as McAfee NSP Sensors), from Intel Corporation, is the Target of Evaluation (TOE). The McAfee NSP Sensors is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

# 2 TOE Description

McAfee NSP Sensors are built for the detection of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks and network misuse.

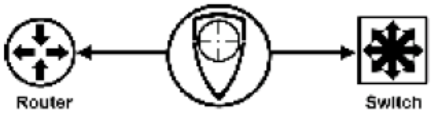
The NSP Sensor component performs:

- Traffic Capture, which captures packets into a data store for review;
- Load balancing and protocol verification, which makes security decisions such that it can filter packets of no interest;
- Denial of Service detection and response; and
- Signature detection and anomaly detection.

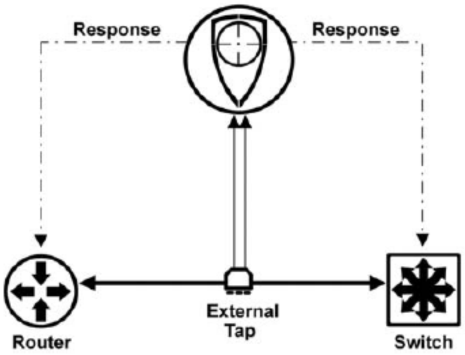
A diagram of the McAfee NSP Sensors architecture is as follows;

The Sensor can operate in three modes:

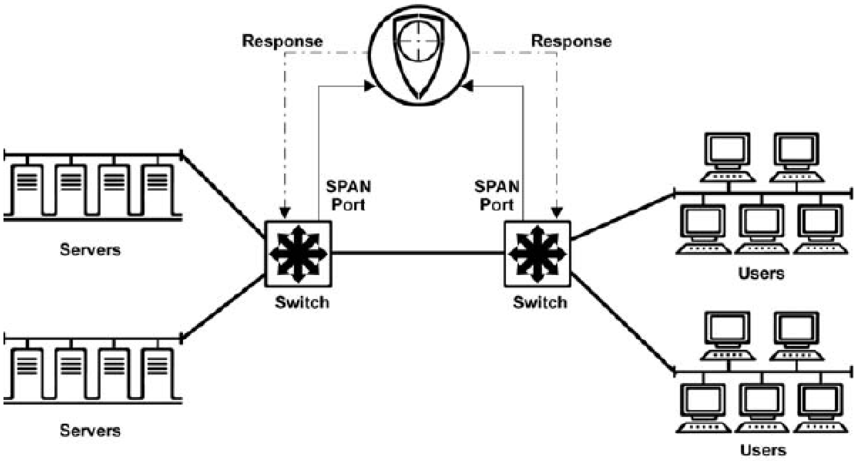
- Inline mode:



- Tap mode:



- Span mode:



## 3 Security Policy

McAfee NSP Sensors implements a role-based access control policy to control administrative access to the system. In addition, McAfee NSP Sensors implements policies pertaining to the following security functional classes:

- Security Audit;
- Cryptographic Support;
- User Data Protection;
- Identification and Authentication;
- Security Management;
- Protection of the TOE Security Functionality (TSF);
- TOE Access; and
- Trusted Path/Channels.

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

| **Cryptographic Module** | **Certificate #** |
|---|---|
| Network Security Platform Sensor M-1250, M-1450, M-2750, M-2850, M-2950, M-3050, M-4050 and M-6050 | 2555 |
| Network Security Platform Sensor M-8000 P | 2558 |
| Network Security Platform Sensor M-8000 S | 2572 |
| Network Security Platform Sensor NS-9100 and NS-9200 | 2591 |
| Network Security Platform Sensor NS-9300 S | 2593 |
| Network Security Platform Sensor NS-9300 P | 2596 |

## 4 Security Target

The ST associated with this Certification Report is identified below:

McAfee Network Security Platform M-Series and NS-Series sensors Version 8.1 Security Target version 1.01, April 8, 2016

## 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.*

McAfee NSP Sensors 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:*

- FAU_STG_EXT.1 - External audit trail storage

- FCS_CKM_EXT.4 - Cryptographic key zeroization
- FCS_RBG_EXT.1 - Cryptographic operation: random bit generation
- 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_EXT.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.

# 6 Assumptions and Clarification of Scope

Consumers of McAfee NSP Sensors 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.

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

## 6.2 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 Evaluated Configuration

The evaluated configuration for McAfee NSP Sensors comprises:

NSP Sensor Software – M-Series v8.1.15.14

Running on one of the following appliances:

| Model Number | Part Number | Revision |
|---|---|---|
| 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-3050 | 600-1246-06-G | F |
| Sensor M-4050 | 600-1245-06-G | F |
| Sensor M-6050 | 600-1220-07-G | E |
| Sensor M-8000 | 600-1221-07-G (Primary)<br>600-1222-07-G (Secondary) | E<br>E |

Or NSP Sensor Software –NS-Series v8.1.17.16

Running on one of the following appliances:

| Model Number | Part Number | Revision |
|---|---|---|
| Sensor NS 9100 | 600-1568-04 | A |
| Sensor NS 9200 | 600-1569-04 | A |
| Sensor NS 9300 | 600-1571-04<br>600-1572-04 | A<br>A |

The publication entitled Network Security Platform 8.1 Common Criteria Evaluated Configuration Guide Revision J describes the procedures necessary to install and operate McAfee NSP Sensors in its evaluated configuration.

# 8 Documentation

The Intel Corporation documents provided to the consumer are as follows:

- IPS Administration Guide Revision A, McAfee Network Security Platform 8.1;
- CLI Guide, Revision A, McAfee Network Security Platform 8.1;

- Network Security Platform 8.1 Common Criteria Evaluated Configuration Guide Revision J;
- M-6050 Sensor Quick Start Guide Revision B, McAfee® Network Security Platform 8.1;
- M-8000 Sensor Quick Start Guide Revision B, McAfee® Network Security Platform 8.1;
- M-2750 Sensor Quick Start Guide Revision B, McAfee® Network Security Platform;
- M-2850/M-2950 Sensor Quick Start Guide Revision B, McAfee® Network Security Platform;
- M-3050/M-4050 Sensor Quick Start Guide Revision B, McAfee® Network Security Platform;
- NS9100, NS9200, NS9300 Sensors Quick Start Guide Revision B, McAfee® Network Security Platform;
- M-2750 Sensor Product Guide Revision B, McAfee® Network Security Platform;
- M-2850/M-2950 Sensor Product Guide Revision C, McAfee® Network Security Platform;
- M-3050/M-4050 Sensor Product Guide Revision B, McAfee® Network Security Platform;
- M-6050 Sensor Product Guide Revision B, McAfee® Network Security Platform;
- M-8000 Sensor Product Guide Revision C, McAfee® Network Security Platform; and
- NS9x00 Sensor Product Guide Revision B, McAfee® Network Security Platform.

# 9 Evaluation Analysis Activities

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

**Development:** The evaluators analyzed the McAfee NSP Sensors functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the McAfee NSP Sensors functional specification is an accurate and complete instantiation of the SFRs.

**Guidance Documents:** The evaluators examined the McAfee NSP Sensors 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 Sensors configuration management system and associated documentation was performed. The evaluators found that the McAfee NSP Sensors configuration items were clearly marked.

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

# 10 ITS Product Testing

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

## 10.1 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 test goals:

a. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP to which the TOE is claiming conformance.

## 10.2 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. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

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

## 10.3 Conduct of Testing

McAfee NSP Sensors was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evalution and Test Facility. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

## 10.4 Testing Results

The independent tests yielded the expected results, providing assurance that McAfee NSP Sensors behaves as specified in its ST and functional specification.

# 11 Results of the Evaluation

This evaluation has provided the basis for an NDPP conformance claim. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

## 12 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 |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| FIPS | Federal Information Processing Standards |
| IT | Information Technology |
| ITSET | Information Technology Security Evaluation and Testing |
| NSP | Network Security Platform |
| PALCAN | Program for the Accreditation of Laboratories - Canada |
| NDPP | Protection Profile for Network Devices |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |

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

e. McAfee Network Security Platform M-Series and NS-Series sensors Version 8.1 Security Target version 1.01, April 8, 2016

f. Evaluation Technical Report for NDPP V1.1 Compliant CC Evaluation of McAfee Inc. McAfee Network Security Platform 8.1, version 1.3, 12 April 2016.