Validation Report

McAfee, Inc.

McAfee Network Security Platform Release 6.1

Document ID: 11-2280-R-0103 V1.1

January 13, 2012

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the McAfee Network Security Platform (NSP) Release 6.1, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the McAfee Network Security Platform (NSP) Release 6.1 Intrusion Detection System (IDS) product was performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States of America (USA) and was completed in October 2011. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR), and the functional testing report. The ST was written by InfoGard Laboratories, Inc. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 July 2009, Evaluation Assurance Level 2 (EAL 2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 r.3, July 2009.

The NSP IDS product 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.

The NSP IDS system is composed of a family of sensor appliances and an NSP management platform referred to as an NSM. The sensor appliances are stand-alone appliances from McAfee, Inc. The sensor appliances are the M-2750, M-1450, M-1250, M-2850, M-2950, M-6050, M-4050, M-8000, M3050, I-4010, I-4000, I-3000, I-2700, I-1400, and I-1200 sensors. All other components of the product are software only components that run on a Windows workstation. The NSM management platform is an IDS management solution for managing NSP sensor appliance deployments for large and distributed enterprise networks. Access to the NSM is supported through a McAfee thick client application installed on a Console Machine. Access to the NSM is authenticated using certificate credentials obtained from a Common Access Card (CAC) in the Operational Environment. Certificates presented are checked for revocation status using an OCSP server in the Operational Environment. The NSM operates with a MySQL Database to persist configuration information and alert data. NSM for Windows Server 2008 includes the MySQL database.

The TOE requires the following software components and supports the following network devices:

Component	Description
Windows Server 2008 SP1	Underlying OS for the NSM Console platform.
Internet Explorer 7 or later	Browser support for establishing Console sessions with NSM.
McAfee Update Server software	Software running on the McAfee update server supporting the TOE with threat signature updates.
Common Access Card software/drivers	Software to support CAC authentication from the NSM Console as applicable based on deployment.
OCSP Server software	OCSP server used to support certificate revocation checking.
NSM Hardware Platform	Hardware Platform for NSM Management Platform capable of running Windows Server 2003/2008; minimum two network interface cards (nic) available.
NSM Software	NSM software installed on the NSM platform.
Console Workstation	Console Platform supporting browser interface used for accessing NSM GUI sessions.
McAfee Update Server hardware	Hardware platform hosting the McAfee threat signature update service.
Common Access Card (CAC) reader hardware	Reader hardware for use with CAC as applicable based on deployment.
OCSP Server hardware	OCSP server hardware used to support certificate revocation checking.
DNS Server	DNS Sever to support Artemis lookups.
NSP Sensor Software	Sensor software installed on McAfee hardware platform.
SSL Certificates (Private Keys)	Used to authenticate to the TOE.

Table 1: Operational Environment

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	McAfee Network Security Platform Release 6.1
Protection Profile	U.S. Government Protection Profile Intrusion Detection System For Basic Robustness Environments, Version 1.7
Security Target	McAfee Network Security Platform (NSP) Security Target
Dates of Evaluation	October 2010 – October 2011
Conformance Result	EAL 2 augmented ALC_FLR.2
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1 R3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1 R3, July 2009
Evaluation Technical Report (ETR)	11-2280-R-0077 V1.1
Sponsor/Developer	McAfee, Incorporated
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Kenji Yoshino, Victor Mendoza, Annie Browne
CCEVS Validators	Olin Sibert, Jean Petty

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before

October 15, 2010.

4 Security Policy

The McAfee Network Security Platform supports the following security policies as described in the Security Target:

4.1 Security Audit

The NSM management platform generates audit records for Administrative sessions and stores them into the MySQL database, running on the same dedicated platform as does the NSM management software. The MySQL Database provides storage and retrieval for audit log information. This function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by the user once authenticated. Auditable actions include changes to the IDS rules and viewing the audit records.

The NSP Sensor also generates audit records based on Sensor detected events and forwards these logs to the NSM platform where they may be integrated into a single (NSP) log resource stored on the MySQL Database platform.

4.2 Cryptographic Operations

The NSP system utilizes symmetric key cryptography to secure communications between TOE components and with the McAfee Update Server in the Operational Environment. Cryptographic services within the Sensor component are provided by a Level 2 FIPS 140-2 validated cryptographic module that includes an OpenSSL implementation. All sessions, except SNMPv3, are conducted using TLSv1 and leverage an OpenSSL Module. Key exchange between the Console browser client and the NSM and between the NSM and NSP Sensor are performed using RSA public/private key exchange. Cryptographic library support is provided for the NSM by RSA BSafe cryptographic libraries and for the NSP Sensor by XySSL library. OpenSSL and both cryptographic libraries are contained within NSP software release packages. When TLS Administration sessions are closed, the OpenSSL module within the Sensor component zeroizes all cryptographic keys used for the sessions. SNMPv3 sessions are secured using the AES algorithm 128 bit key size.

4.3 Identification and Authentication

An X.509 certificate (derived from a CAC) is passed to the NSM during the session negotiation process and, within that certificate, a Common Name (CN) that is extracted and checked against a user list on the NSM. The certificate also is required to be signed by a trusted CA as configured during NSP system installation.

4.4 Security Management

The NSM provides a detailed security management interface used to configure and manage the NSP TOE as well as provide a report and analysis utility for investigating traffic events.

4.5 Protection of the TSF

The McAfee Sensors and NSM management platform all protect TSF data from disclosure and modification, when it is transmitted between separate parts of the TOE, by communicating using TLS version 1.0 connections.

The Sensor communicates with the NSM management platform through its dedicated 10M/100M Ethernet port using TCP/IP. This communication uses secure channels; providing link privacy using encryption and mutual authentication with public key authentication.

4.6 System Data Collection

The collection subsystem is used to detect events while monitoring the target network. Upon detection of such events, the collection subsystem generates data which is sent to the NSM for storage in the system database. For each event detected, the collection subsystem records and the NSM stores the date and time of the event, type of event, subject identity and the outcome (success or failure) of the event with additional details for each event.

The NSM allows Security Administrators to establish new rules to detect new vulnerabilities, allowing complete control over the types of traffic that will be monitored and to set rules to govern the collection of data regarding potential intrusions.

For Network Traffic Events, the Protocol, Source Address and Destination Addressed are collected in audit records. For Vulnerability Detection Events, the identifier of the known vulnerability is listed in the audit records.

4.7 System Data Analysis

The TOE provides many pre-configured rule sets and policies for immediate application in a number of different network areas. Each pre-configured policy is matched with an identically named rule set designed to address the common attacks targeting specific network environments. Existing rule sets cannot be modified but they may be “cloned” and then modified to create a custom rule set.

Data Analysis is conducted using threat signatures that contain characteristics know to be representative of malicious traffic, malware, virus, or worm infections. A series of threat signatures are provided and regularly updated to allow the NSP TOE to identify potentially malicious traffic. In addition, the User Defined Signature feature allows authorized administrators to develop custom signatures and use them for traffic analysis.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

A.NTRSRC An OCSP Server, McAfee Update Server, and a DNS server will be available in the Operational Environment.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

T.EAVESDROP A malicious user or process may observe or modify TSF data transmitted between a separate part of the TOE or between the TOE and a trusted IT Entity.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.SCNCFG	Improper security configuration settings may exist in the IT System that the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modifications of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P. SYSADMIN	The NSM platform shall be configured such that only the Security Administrator user has access to the underlying Operating System file system.

6 Architectural Information

The TOE is classified as an Intrusion Detection System (IDS) for Common Criteria purposes. The TOE is made up of *hardware and software* components. The TOE consists of three main components that are: the NIC, the NSP sensor(s) appliance, and the Network Security Manager. The NIC is outside of the TOE boundary.

6.1 NSP Sensors

NSP sensors are content processing appliances that perform stateful inspection on a packet basis to discover and prevent intrusions, misuse, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks. McAfee, Inc. offers various types of sensor appliances providing different bandwidth and deployment strategies:

M-Series	I-Series
M-8000	I-4010
M-6050	I-4000
M-4050	I-3000
M-3050	I-2700
M-2750	I-1400
M-2850	I-1200
M-2950	
M-1450	
M-1250	

6.2 Network Security Manager (NSM)

The Network Security Manager consists of software that is used to configure and manage an NSP deployment. The NSM is a set of applications coupled with an embedded MySQL Database. The MySQL Database is installed during NSM installation and is configured so that it can be accessed only by the NSM application. The MySQL Database must reside on the same platform as does the NSM. The Network System Manager (NSM) is available in three versions: NSM Global Manager, NSM Standard Manager, and NSM Starter Manager. All versions of the NSM are part of the TOE and part of the same core software release. All versions of the NSM operate within an Operational Environment composed of an Intel-based hardware platform with a Windows Server 2008 operating system (OS). The difference between the three versions is one of scalability. The NSM Starter Manager supports up to 2 NSP Sensors, the NSM Standard Manager supports up to 6 NSP sensors, and the NSM Global Manager supports an unlimited number of NSP sensors of any type or combination.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Network Security Platform. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is physically delivered to the End-User. The guidance documents are provided for download with the TOE software in accordance with EAL 2 requirements from the McAfee support website and apply to the CC Evaluated configuration:

7.1 Design Documentation

Document	Revision	Date
IntruShield TOE Design Document (ADV_TDS)	1.0	July 2, 2011
Network Security Platform (NSP) Functional Specification Document (ADV_FSP)	1.0	July 2, 2011
Network Security Platform (NSP) version 6.1 TOE Security Architecture (ADV_ARC)	1.0	July 7, 2011

7.2 Guidance Documentation

Document	Revision	Date
Network Security Platform (NSP) version 6.1 Common Criteria Supplement EAL2 + ALC_FLR.2	1.1	January 11, 2012
Getting Started Guide revision 5.0 **McAfee® Network Security Platform Version 6.0**	700-2365-00/ 4.0	November 2010
Release Notes – Network Security Platform	700-2360E00	December 13, 2010
IPS Configuration Guide revision 1.0 **McAfee® Network Security Platform version 6.0**	700-2372-00/ 1.0	September 2010
IPS Deployment Guide revision 2.0 **McAfee® Network Security Platform version 6.0**	700-2366-00/ 2.0	November 2010

Document	Revision	Date
System Status Monitoring Guide revision 3.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2375-00/ 3.0	September 2010
Network Security Platform® M-6050 Quick Start Guide	700-2398-00	N/A
Network Security Platform® M-8000 Quick Start Guide	700-2400-00	N/A
Network Security Platform M-1250/M-1450 Quick Start Guide	700-2396-00	N/A
Network Security Platform M-2750 Quick Start Guide	700-2392-00	N/A
Network Security Platform M-2850/M-2950 Quick Start Guide	700-2651C00	N/A
Network Security Platform® M-3050/M-4050 Quick Start Guide	700-2394-00	N/A
Intrushield I-2700 Quick Start Guide	700-1063-03-G	N/A
Intrushield I-4010, I-3000 Quick Start Guide 2.1	700-1013-03-G	N/A
Intrushield I-4000 Quick Start Guide 2.1	700-1261-00-G	N/A
Intrushield I-1200, I-1400 Quick Start Guide 2.1	700-1259-00-revB	N/A
Administrative Domain Configuration Guide revision 3.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2368-00/ 3.0	September 2010
Best Practices Guide revision 6.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2379-00/ 6.0	December 2010
Manager Configuration Basics Guide revision 2.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2367-00/ 2.0	September 2010

Document	Revision	Date
Reports Guide revision 3.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2376-00/ 3.0	September 2010
Special Topics Guide - Virtualization revision 1.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2383-00/ 1.0	December 2009
Troubleshooting Guide revision 5.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2380-00/ 5.0	September 2010
Custom Attack Definitions Guide revision 1.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2377-00/ 1.0	December 2009
M-1250/M-1450 Sensor Product Guide revision 2.0	700-2395-00/ 2.0	March 2010
M-2750 Sensor Product Guide revision 3.0	700-2391-00/ 3.0	December 2010
M-2850/M-2950 Sensor Product Guide revision 1.0	700-2652-00 1.0	January 2011
M-3050/M-4050 Sensor Product Guide revision 2.0	700-2393-00/ 2.0	January 2010
M-6050 Sensor Product Guide revision 2.0	700-2397-00/ 2.0	January 2010
M-8000 Sensor Product Guide revision 2.0	700-2399-00-G/ 2.0	January 2010
NSP Sensor I-4010 Product Guide revision 2.0	700-2390-00/ 2.0	January 2010
NSP Sensor I-4000 Product Guide revision 1.0	700-2389-00/ 1.0	December 2009
NSP Sensor I-3000 Product Guide revision 2.0	700-2388-00/ 2.0	January 2010
NSP Sensor I-2700 Product Guide revision 1.0	700-2387-00/ 1.0	December 2009
NSP Sensor I-1400 Product Guide revision 2.0	700-2386-00/2.0	May 2010

Document	Revision	Date
NSP Sensor I-1200 Product Guide revision 2.0	700-2385-00/ 2.0	May 2010
CLI Guide Revision 2.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2370-00/ 2.0	December 2010
Device Configuration Guide Revision 4.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2371-00/ 4.0	November 2010
Installation Guide revision 5.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2252-00/ 5.0	November 2010
Manager Server Configuration Guide revision 2.0 **McAfee® Network Security Platform Network Security Manager version 6.0**	700-2369-00/ 2.0	November 2010
Addendum III to 6.1 Documentation revision 1.0	700-2655-00/ 1.0	April 2011
Integration Guide revision 4.0	700-2374-00/ 4.0	October 2010
McAfee Network Security Platform FIPS Label Placement Procedure (Applicable for M-6050 and M-4050)	700-2270-00	N/A
McAfee Network Security Platform FIPS Label Placement Procedure (Applicable for M-3050)	700-2271-00	N/A
McAfee Network Security Platform FIPS Label Placement Procedure (Applicable for M-1450 and M-1250)	700-2272-00	N/A
McAfee Network Security Platform FIPS Label Placement Procedure (Applicable for M-2750)	700-2346-00	N/A
McAfee Network Security Platform FIPS Label Placement Procedure (Applicable for M-8000)	700-2356-00	N/A

7.3 Configuration Management and Lifecycle

Document	Revision	Date

Document	Revision	Date
EAL 2 + ALC_FLR.2 Life Cycle Support Documentation McAfee® Network Security Platform (NSP) Intrusion Detection System Configuration Management ALC_CMS.2, ALC_CMC.2	1.1	January 11, 2012
McAfee® Network Security Platform (NSP) Common Criteria Secure Delivery Document EAL 2 augmented ALC_FLR.2	1.0	October 10, 2011
EAL 2 Flaw Reporting Procedures McAfee® Network Security Platform (NSP) Intrusion Detection System augmented ALC_FLR.2	1.0	December 7, 2010

7.4 Test Documentation

Document	Revision	Date
McAfee Network Security Platform Test (ATE) Document	1.3	October 10, 2011
Independent and Penetration Test Plan	1.1	October 4, 2011

7.5 Vulnerability Assessment Documentation

Document	Revision	Date
McAfee Network Security Platform (NSP) Common Criteria Vulnerability Analysis AVA_VAN.2 EAL2	1.2	October 11, 2011

7.6 Security Target

Document	Revision	Date
McAfee® Network Security Platform (NSP) Security Target	1.1	January 10, 2012

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces along with test tools to simulate attacks and alerts.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results are also included in the TOE Test Plan. The Developer testing effort tested the available interfaces to the TSF.

The Evaluation Team verified that the Developer's testing tested aspects of the SFRs defined in the ST. This analysis ensures adequate coverage for EAL 2. The Evaluation Team determined that the Developer's actual test results matched the Developer's expected test results.

8.2 Evaluation Team Independent Testing

The Evaluation Team conducted independent testing of the TOE. The Evaluation Team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The Evaluation Team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The Evaluation Team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation Team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The Evaluation Team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions not extensively tested by the developer's tests
- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions with open parameters (e.g. text fields, unbounded number fields)

The Evaluation Team conducted 12 of the Developer's test cases and specified 11 independent tests and 6 penetration tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once and the Evaluation Team verified that each test passed.

8.3 Vulnerability Analysis

The Evaluation Team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Evaluation Team's vulnerability analysis and penetration tests.

The Evaluators performed a vulnerability analysis of the TOE to identify any obvious vulnerabilities in the product and to determine if they are exploitable in the intended

environment for the TOE operation. In addition, the Evaluation Team performed a public domain search for potential vulnerabilities. The public domain search did not identify any known vulnerabilities in the TOE as a whole or any components of the TOE.

Based on the results of the Evaluation Team's vulnerability analysis, the Evaluation Team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with Basic attack potential. The Evaluation Team conducted testing using the same test configuration that was used for the independent testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing and the design activity to devise the penetration tests. The penetration tests attempted to misuse components of the TOE (e.g., directly access the MySQL database) and put the TOE in undefined states. This resulted in a set of four penetration tests.

9 Evaluated Configuration

The Evaluated Configuration consists of the NSM software installed on a dedicated Windows Server 2003 SP3 or Windows Server 2008 SP1 platform and an NSP Sensor.

The Sensor models that may be used as part of an evaluated configuration are models M-2750, M-1450, M-1250, M-6050, M-4050, M-8000, M-3050, M-2850, M-2950, I-4010, I-4000, I-3000, I-2700, I-1400, and I-1200.

NSM version 6.1.15.17 was evaluated. M series sensor software version 6.1.15.35 was evaluated. I series sensor software version 6.1.1.7 was evaluated.

The communications between NSM and Sensors must be performed on an isolated network. An administrative console running Internet Explorer 7 or later and CAC authentication hardware and software is also required.

NSM requires connectivity to an OCSP server and the McAfee Update Server.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 + ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in October 2011.

11 Validator Comments/Recommendations

The TOE was successfully evaluated in the defined evaluated configuration and scope described in sections 9 and 10 of this Validation Report. The validation team recommends certification of the TOE at EAL 2 augmented with ALC_FLR.2.

The validators noted that during testing, it was determined that malware scanning was not effective on partial files because the malware signature scan applies only to complete files. If part of a known malware file is downloaded in one transaction, and the remainder of the file is downloaded in a second transaction, the file is not identified as malware. This type of partial-file download can occur in normal user operations with a web browser (e.g., Internet Explorer 7), which retains the first part of a partly downloaded file and only asks for the remaining part when the download is retried. Because malware scanning allows the file to be transferred until the point at which it is detected as malware, the browser actually receives most of the file before the IDS interrupts its transfer. Thus, when the browser tries to download the file again, it picks up where the earlier download was interrupted.

This effect is an unavoidable in network-based file scanning, and does not represent a failure of the TOE. When this scenario occurs, a security alert is generated and logged after the first partial transfer (when the malware is detected), and also after the second transfer, because the partial transfer is considered a reportable anomaly.

12 Security Target

McAfee Network Security Platform (NSP) Security Target, Version 1.1, January 10, 2012.

13 Terms

13.1 Glossary

Alert	An alert is a notification of a system event, attack, or other incident that triggers the Intrusion Detection System.
Authorized Administrator(s)	A general term used to refer to administrative users holding the Security Administrator, Audit Administrator, or Crypto Administrator roles.
Attack	A set of actions performed by an attacker that poses a threat to the security state of a protected entity in terms of confidentiality, integrity, authenticity, availability, authorization, and access policies.
CIDR	(Classless Inter-Domain Routing) A scheme which allocates blocks of Internet addresses in a way that allows summarization into a smaller number of routing table entries. A CIDR address contains the standard 32-bit IP address but includes information on how many bits are used for the network prefix. For example, in the CIDR address 123.231.121.04/22, the "/22" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host.
Denial of Service	In a Denial of Service (DoS) attack, the attacker attempts to crash

	a service (or the machine), overload network links, overload the CPU, or fill up the disk. The attacker does not always try to gain information, but to simply act as a vandal to prevent you from making use of your machine. Ping floods and Smurf attacks are examples of DoS attacks.
Distributed DDoS	These attacks usually consist of standard DoS attacks Denial of orchestrated by attackers covertly controlling many, sometimes hundreds, of different machines.
HTTPS	The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using Secure Socket layer (SSL) or Transport Layer Security (TLS) encryption.
Intrusion	Unauthorized access to, and/or activity in, an information system, usually for the purpose of tampering with or disrupting normal services. See also Attack.
Intrusion Detection	The process of identifying that an intrusion has been attempted, is occurring, or has occurred.
NTP	Network Time Protocol provides a mechanism to synchronize time on computers across the internet. The specification for NTP version 3 is defined in RFC 1305. Such synchronization can be very useful for multi-machine activities that depend upon accurate time stamps.
Policy	A user-configured security rule that determines the permission of traffic across a network. Policies can set rules for protocols (HTTP, UDP), machines (NT, Solaris), operating systems (Unix), and other types of network information. A policy also defines what actions should be taken in the event of non-permissible activity.
Policy Violations	All activities for which the underlying traffic content may not be malicious by itself, but are explicitly forbidden by the usage policies of the network as defined by a security policy. These can include “protocol violations” wherein packets do not conform to network protocol standards. (For example, they are incorrectly structured, have an invalid combination of flags set, or contain incorrect values.) Examples might include TCP packets with their SYN and RST flags enabled, or an IP packet whose specified length doesn’t match its actual length. A protocol violation can be an indication of a possible attack, but can also be triggered by malfunctioning software, hardware or could be applications/protocols forbidden in the network (e.g. Peer to Peer (P2P)).

Port Cluster	Port Cluster is a more intuitive term for an Interface Group. An interface group enables multiple sensor ports to be grouped together for the effective monitoring of asymmetric environments. Interface groups normalize the impact of traffic flows split across multiple interfaces, thus maintaining state to avoid information loss. Once configured, an interface group appears in the Resource Tree as a single interface node (icon) under the sensor where it is located. All of the ports that make up the interface are configured as one logical entity, keeping the configuration consistent.
MySQL Database	A Relational database that allows the definition of data structures, storage/retrieval operations, and integrity constraints. The data and relations between them are kept in organized tables, which are collections of records and each record in a table contains the same fields.
Roles	A class of user privileges that determines the authorized activities of the various users in the system.
Sensor	The sensor is a network device containing the intrusion detection engine. It analyzes network traffic, searching for signs of unauthorized activity.
Signature	Activities or alterations to an information system indicating an attack or attempted attack, detectable by examination of audit trail logs.
Span Mode	One of the monitoring modes available for an NSP sensor. In Span Mode, the sensor functions by mirroring the packet information on a switch or hub and sending the information to a sensor for inspection, while continuing the transmission of traffic with negligible latency. SPAN mode is typically half-duplex, and works through a connection of a sensor to a port on a hub or the SPAN port of a switch.
SPAN Port	On a switch, SPAN mirrors the traffic at one switched segment onto a predefined port, known as a SPAN port.
Threat Analyzer	A graphical user interface for viewing specific attack information in the NSM System. The Threat Analyzer interface is part of the NSM component, and focuses on alert forensic analysis.
TLS	A secure socket layer (TLS) is an encryption protocol invoked on a Web server that uses HTTPS.
Tap	A tap is hardware device that passes traffic unidirectionally from a network segment to the IDS. Traffic is mirrored as it passes through the tap. This mirror image is sent to the IDS for

	inspection. This prevents traffic passing from being directed at the IDS.
Tap Mode	One of the monitoring modes available for an NSP sensor. Functions by mirroring the packet information and sending the information to a sensor for inspection, while continuing the transmission of traffic with negligible latency. Tap mode works through installation of an external wire tap, a port on a hub, the SPAN port of a switch, or through an internal tap when deploying the I-2600. Also known as passive monitoring mode.
Virtual IDS	An NSM feature that enables you to logically segment a sensor into a large number of virtual sensors, each of which can be customized with its own security policy. Virtual IDS (VIDS) are represented in the NSM as *interfaces* and *sub-interfaces*.
VLAN	Virtual Local Area Network. A logical grouping of two or more nodes which are not necessarily on the same physical network segment, but which share the same network number. This is often associated with switched Ethernet networks.
Vulnerability	Any characteristic of a computer system that will allow someone to keep it from operating correctly, or that will let unauthorized users take control of the system.

13.2 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
NSM	Network Security Manager
NSP	Network Security Platform (TOE system)
OCSP	Online Certificate Status Protocol
PP	Protection Profile

SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.