National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Intel Corporation

2821 Mission College Blvd.

Santa Clara, CA 95054

Intel Corporation McAfee Advanced Threat Defense

Report Number: CCEVS-VR-10622-2014
Dated: May 27, 2015
Version: 0.3

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Common Criteria Testing Laboratory

Tammy Compton
Chris Keenan
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of McAfee Advanced Threat Defense solution provided by Intel Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in May 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1.

The Target of Evaluation (TOE) is the McAfee Advanced Threat Defense models 3000 and 6000 running software version 3.4.6 products. The TOE is a hardware network appliance. The product provides a web interface over TLS and a console connection.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the – Intel Corporation McAfee Advanced Threat Defense (NDPP11e3) Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 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 Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Intel Corporation McAfee Advanced Threat Defense models 3000 and 6000 running software version 3.4.6
Protection Profile	Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) (including the optional TLS requirements) with Errata #3
ST:	Intel Corporation McAfee Advanced Threat Defense (NDPP11e3) Security Target, Version 0.5, May 22, 2015
Evaluation Technical Report	Evaluation Technical Report for McAfee Advanced Threat Defense (NDPP11e3), Version 0.3, May 27, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Intel Corporation
Developer	Intel Corporation

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is **Error! Reference source not found.** (MATD). MATD detects today's stealthy, zero-day malware with layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior.

The MATD hardware appliance implements dynamic and statistical analysis on data transmitted through a network to provide malware detection, assessment and classification.

The MATD processes the files through the down selectors for statistical analysis and provides a sandbox test environment which includes virtual machines running customer environments, anti-virus, anti-malware, local blacklist and whitelists. Files are executed within virtual machine environments that are monitored by the log file. The log file is then used to generate a security report of the potential malware.

For the purpose of evaluation, MATD will be treated as a network device offering CAVP certified cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records)

3.1 TOE Evaluated Platforms

The evaluated configuration of consists of McAfee Advanced Threat Defense with software version 3.4.6 running on one of the following modules:

- ATD-6000: McAfee Advanced Threat Defense 6000
- ATD-3000: McAfee Advanced Treat Defense 3000

3.2 Physical Boundaries

The ATD evaluated configuration includes software version 3.4.6 running on one of the following modules:

- ATD-6000: McAfee Advanced Threat Defense 6000, 2U 4x Xeon E5-4640 (2.5GHz), 256GB DDR3, 16TB of HDD storage and 1600MB of SSD storage.
- ATD-3000: McAfee Advanced Treat Defense 3000, 1U 2x Xeon E5-2658 (2.1GHz), 192GB DDR3, 8TB of HDD storage and 800MB of SSD storage

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an external NTP server in the operational environment.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security Management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

4.1 Security audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log or export them to a syslog server using a TLS protected channel.

4.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its TLS implementation. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

4.3 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets

4.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes.

4.5 Security management

The TOE provides a command line (CLI) management interface as well as a graphical user interface (GUI) accessed via the web. The web interface is protected with TLS. The management interface is limited to the authorized administrator (as defined by a role).

4.6 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It provides a hardware clock to ensure reliable timestamps. It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an authorized administrator.

4.7 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

4.8 Trusted path/channels

The TOE provides a local console which is subject to physical protection. For remote access, the web GUI is protected by TLS thus ensuring protection against modification and disclosure.

The TOE also protects its audit records from modification and disclosure by using TLS to communicate with the syslog server.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP). That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- NDPP Admin Guide, v 3.4.6, 5/20/15
- ATD 3.4.6 Product Guide, Revision A

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the McAfee Advanced Threat Defense, Version 1.3, May 25, 2015.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the NDPP Admin Guide, v 3.4.6, 5/20/15 document and ran the tests specified in the NDPP including the optional TLS tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, consists of McAfee Advanced Threat Defense with software version 3.4.6 running on one of the following modules:

- ATD-6000: McAfee Advanced Threat Defense 6000, 2U 4x Xeon E5-4640 (2.5GHz), 256GB DDR3, 16TB of HDD storage and 1600MB of SSD storage.
- ATD-3000: McAfee Advanced Treat Defense 3000, 1U 2x Xeon E5-2658 (2.1GHz), 192GB DDR3, 8TB of HDD storage and 800MB of SSD storage

To use the product in the evaluated configuration, the product must be configured as specified in the NDPP Admin Guide, v 3.4.6, 5/20/15 document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL1 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon

CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the **Error! Reference source not found.** models 3000 and 6000 running software version 3.4.6 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

This section is used to impart additional information about the evaluation results. These comments/ recommendations can take the form of shortcomings of the IT product discovered during the evaluation or mention of features which are particularly useful.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Intel Corporation McAfee Advanced Threat Defense (NDPP11e3) Security Target, Version 0.5, May 22, 2015*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP).