National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Trend Micro TippingPoint Threat Protection System (TPS) v5.1

Report Number:	**CCEVS-VR-VID10949-2019**
Dated:	**30 January 2019**
Version:	**1.0**

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

Paul Bicknell, Senior
John Butterworth, Lead
Michelle Carlson
Stelios Melachrinoudis, Lead
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review 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 and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Trend Micro TippingPoint Threat Protection System (TPS) v5.1 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Trend Micro TippingPoint Threat Protection System (TPS) v5.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in January 2019.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 ([1], [2], [3], [4]) and activities specified in the following document:

- Evaluation Activities for Network Device cPP, Version 2.0 + Errata 20180314, March 2018 [6]

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The product comprises network appliances and virtual appliances on specified hardware used to facilitate threat protection, shield computing infrastructure from network vulnerabilities, block exploits, and defend against known and zero-day attacks. The focus of the evaluation was on the product's conformance to the security functionality specified in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018 [5]

The security functions specified in this Protection Profile include protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([13]) and the associated test report produced by the Leidos evaluation team ([15]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6] had been performed appropriately. 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.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0259: NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187
- TD0260: NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4
- TD0290: NIT technical decision for physical interruption of trusted path/channel
- TD0291: NIT technical decision for DH14 and FCS_CKM.1
- TD0334: NIT Technical Decision for Testing SSH when password-based authentication is not supported.
- TD0336: NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8
- TD0337: NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6
- TD0338: NIT Technical Decision for Access Banner Verification
- TD0339: NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2

All other Technical Decisions were found to be not applicable to the TOE, either because they were not related to the claimed Protection Profile or because they related to optional or selection-based functionality that was not claimed in the TOE's Security Target [7].

1.2 Threats

The Security Problem Definition, including the threats, may be found in the collaborative Protection Profile for Network Devices, Version 2.0 +.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 Product Compliant List (PCL).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Trend Micro TippingPoint Threat Protection System (TPS) v5.1
Sponsor & Developer:	Trend Micro, Inc. 11305 Alterra Parkway Austin, TX 78758
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	January 30, 2019
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Anthony Apted Greg Beaver Justin Fisher Allen Sant Kevin Steiner
Validation Personnel:	Paul Bicknell John Butterworth Michelle Carlson Stelios Melachrinoudis

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the ETR.

3.1 Security Audit

The TOE is able to generate audit records for security relevant events specified in the claimed PP. The TOE can be configured to store the audit records locally on the TOE and can also be configured to send the logs to a designated external log server. The audit records in local audit storage cannot be modified or deleted. In the event the space available for storing audit records locally is exhausted, the TOE deletes the oldest historical log file, renames the current log file to be a historical file, and creates a new current log file. The TOE will write a warning to the audit trail when the space available for storage of audit records exceeds 75% space remaining threshold.

3.2 Cryptographic Support

The TOE is operated in FIPS mode and includes FIPS-approved and NIST-recommended cryptographic algorithms. The TOE provides cryptographic mechanisms for symmetric encryption and decryption, cryptographic signature services, cryptographic hashing services, keyed-hash message authentication services, deterministic random bit generation seeded from a suitable entropy source, and key zeroization. The cryptographic mechanisms support SSH used for secure communication, both as client and server.

3.3 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and a network accessible interface over SSH to support administration of the TOE.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. When a user is authenticated at the local console, no information about the authentication data (i.e., password) is echoed to the user. Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: !; @; #; $; %; ^; &; *; (;); ,; .; ?; <; >; and /.

The TOE provides authentication failure handling for remote administrator access. When the defined number of unsuccessful authentication attempts has been reached, the remote administrator accessing the TOE via SSH is locked out for an administrator configurable period of time. Authentication failures by remote Administrators cannot lead to a situation where no Administrator access is available to the TOE since administrator access is still available via local console.

3.4 Security Management

The TOE provides administrator roles and supports local and remote administration. The TOE supports Super User, Admin, and Operator roles that map to the Security Administrator role in the protection profile. Each user must be assigned a role in order to perform any management action.

3.5 Protection of the TSF

The TOE protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism that ensures reliable time information is available.

The TOE provides mechanisms to view the current version of the TOE and to install updates of the TOE software. TOE updates are initiated manually by the Super User or Admin, who can verify the integrity of the update prior to installation using a digital signature.

The TOE performs tests for software module integrity and cryptographic known-answer tests.

3.6 TOE Access

The TOE implements administrator-configurable session inactivity limits for local interactive sessions at the console and for SSH sessions. The TOE will terminate such sessions when the inactivity period expires. In addition, administrators can terminate their own interactive sessions by logging out at the console and SSH.

The TOE supports an administrator-configurable TOE access banner that is displayed prior to a user completing the login process at the CLI. This is implemented for both local and remote management connections (console, SSH).

3.7 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH. SSH ensures confidentiality of transmitted information and detects any loss of integrity.

The TOE also uses SSH to protect the transmission of audit records to an external audit server.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, are as follows:

- The device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.
- The device is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent of the functionality that is evaluated for conformance to the NDcPP is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data.
- The authorized administrators for the device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
- The device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Evaluation Activities for Network Device cPP* [6] and performed by the evaluation team).
- This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Trend Micro TippingPoint Threat Protection System (TPS) v5.1 Security Target, Version 1.0, January 11, 2019 [7].
- Only the following protocols implemented by the product have been tested, and only to the extent specified by the security functional requirements: SSH.

- The TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- The TOE can be configured to use the following components in its operational environment, however, these components have not been evaluated and their use with the TOE is not covered by this evaluation:
    - Administrator workstation—computer connected either directly or remotely to the appliance's Management port via an RJ-45 Ethernet cable. The Management port is an out-of-band management port that provides access to the CLI via SSH.
    - syslog server
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.
- The evaluated configuration comprises individual TPS devices managed in isolation, and not a distributed solution. Additionally, when deploying the TOE in a virtualized environment, the VM-Series virtual appliance must be the only guest running in the virtualized environment, and no other non-network applications may be running on the VM.

5 TOE Evaluated Configuration

5.1 Evaluated Configuration

Trend Micro TippingPoint Threat Protection System (TPS) v5.1, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report. The specific appliance models include:

- TPS 440T
- TPS 2200T (1 Gbps)
- TPS 2200T (2 Gbps)
- TPS 8200TX
- TPS 8400TX
- vTPS

The vTPS model was tested using both VMware ESXi v6.5 and RHEL KVM v7.1. The host platforms for the VM hypervisors were tested using Intel Xeon processors.

The vTPS virtual appliance must be the only guest running in the virtualized environment, in accordance with the requirements of the NDcPP.

5.2 Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the NDcPP is excluded from the evaluation scope. The product also has the following exclusions:

- The TippingPoint Threat Protection System product includes a Local Security Management (LSM) component that provides remote administrative management. The LSM is a GUI over HTTPS. In the evaluated configuration, all management must be performed using the CLI.
- The TPS devices can be configured to use sFlow record emission to sample a random flow of traffic and send the data to a collector server for analysis. SFlow and collector services are not in the evaluated configuration.
- Two TippingPoint Threat Protection appliances can be installed in a redundant network configuration. This system configuration provides High Availability (HA), ensuring that the network traffic always flows at wire speeds in the event of any internal hardware or software failure on the device. HA is not included in the evaluated configuration.
- TippingPoint Threat Protection appliances can be installed in a stacking configuration. Stacking enables an increase in the overall inspection capacity of TPS by grouping multiple TX Series devices and pooling their resources. Stacking configurations are not included in the evaluated configuration.
- Optional bypass I/O modules are available for the 8200TX and 8400TX security devices that provide high availability for copper and fiber segments. These modules are not included in the evaluated configuration.

6 Documentation

Trend Micro offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with each TOE model is as follows:

- Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, Version 5.1, July 2018 [9]
- Trend Micro TippingPoint Threat Protection System (TPS) Command Line Interface reference, October 2018 [8]
- Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.1, Version 1.0, 11 January 2019 [13]

The following guidance is also provided for initial setup purposes, but it is only necessary to reference the guidance that relates to the specific TOE model(s) being installed:

- Trend Micro TippingPoint Threat Protection System Install Your 440T and 2200T Security Devices, Revision 6, July 2018 [10]
- Trend Micro TippingPoint Threat Protection System Install Your 8200TX and 8400TX Security Devices, Revision 2, July 2018 [11]
- Trend Micro TippingPoint Virtual Threat Protection System (vTPS) Deployment Guide, Version 5.1, July 2018 [12]

To use the product in the evaluated configuration, the product must be configured as specified in these guides.

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download this CC configuration guide (CCECG above) from the NIAP website.

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary documents:

- *Trend Micro TippingPoint Threat Protection System (TPS) v5.1 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.0* [14]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for Trend Micro TippingPoint Threat Protection System (TPS) [15]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to *collaborative Protection Profile for Network Devices* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *collaborative Protection Profile for Network Devices* [5]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* [5] were fulfilled.

7.1 Test Configuration

The evaluated version of the TOE consists of Trend Micro TippingPoint Threat Protection System (TPS) 5.1 running on any of the following physical and virtual appliances:

- TPS 440T
- TPS2200T
- TPS8200TX
- TPS8400TX
- vTPS

The TOE must be deployed as described in section 4.1 of this Validation Report and be configured in accordance with the *Trend Micro TippingPoint Threat Protection System (TPS) Command Line Interface reference* [8] and *Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.1* [13].

7.2 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profiles and using the flaw-hypothesis methodology. This included a search of public vulnerability databases and development of Type 3 flaw hypotheses in accordance with Section A.3 of [6]. These searches were performed during the evaluation and then re-performed a final time on

November 30, 2018 to ensure that no additional public vulnerabilities were disclosed prior to the completion of the evaluation.

The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and several other public vulnerability repositories.

The keyword searches included the following terms:

- “TippingPoint”
- “threat protection”
- “TCP”
- “SSH”
- “openssh” – specifically, only results for version 7.5p1 or newer were considered
- “openssl” – specifically, only results for version 1.0.2l or newer were considered
- “Linux” – specifically, only results for version 4.4.85 or newer were considered

The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 4 of the CC and CEM:

- *Evaluation Activities for Network Device cPP*, Version 2.0 + Errata 20180314, March 2018 [6]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). As stated in the Clarification of Scope, the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable

11 Security Target

The ST for this product's evaluation is *TippingPoint Threat Protection System (TPS) v5.1 Security Target*, Version 1.0, 11 January 2019 [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13 Bibliography

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

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

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, 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 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018

[6] Evaluation Activities for Network Device cPP, Version 2.0 + Errata 20180314, March 2018

[7] Trend Micro TippingPoint Threat Protection System (TPS) v5.1 Security Target, Version 1.0, January 11, 2019

[8] Trend Micro TippingPoint Threat Protection System (TPS) Command Line Interface reference, October 2018

[9] Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, Version 5.1, July 2018

[10] Trend Micro TippingPoint Threat Protection System Install Your 440T and 2200T Security Devices, Revision 6, July 2018

[11] Trend Micro TippingPoint Threat Protection System Install Your 8200TX and 8400TX Security Devices, Revision 2, July 2018

[12] Trend Micro TippingPoint Virtual Threat Protection System (vTPS) Deployment Guide, Version 5.1, July 2018

[13] Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.1, Version 1.0, 11 January 2019

[14] Trend Micro TippingPoint Threat Protection System (TPS) v5.1 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.0, January 11, 2019

[15] Assurance Activities Report for Trend Micro TippingPoint Threat Protection System (TPS), Version 1.1, January 11, 2019