National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Trend Micro TippingPoint Threat Protection System (TPS) v5.3

Report Number: CCEVS-VR-VID11206-2022
Dated: February 2, 2022
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Daniel Faigin
Swapna Katikaneni
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Trend Micro TippingPoint Threat Protection System (TPS) v5.3 (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 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 VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in February 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant and meets the assurance requirements of the *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The TOE is Trend Micro TippingPoint Threat Protection System (TPS) v5.3.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR 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 documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed PP and, when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([7]). The technical information included in this report was obtained from the Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Security Target, version 1.0, 2022/01/01 and analysis performed by the Validation Team.

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 (CC) 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).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules 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	Trend Micro TippingPoint Threat Protection System (TPS) v5.3
Security Target	Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Security Target, Version 1.0, 1 January 2022
Sponsor & Developer	Trend Micro 11305 Alterra Parkway Austin, TX 78758
Completion Date	February 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Evaluation Personnel	Anthony Apted Pascal Patin Allen Sant
Validation Personnel	Daniel Faigin Swapna Katikaneni

3 TOE Architecture

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

The TOE consists of the TPS 1100TX, TPS 5500TX, TPS 8200TX, and TPS 8400TX hardware appliances, and the vTPS virtual appliance. Each appliance is a standalone network device.

Each TOE hardware appliance includes an RJ-45 console port, a 1 GbE copper management port, and one or more standard I/O modules used to receive and transmit packets for the threat detection functions. The 1100TX includes one I/O module slot, the 5500TX and the 8200TX include two I/O module slots, and the 8400TX includes four I/O module slots. The 8200TX and 8400TX devices are high-end systems that are designed for network environments requiring up to 40 Gbps of inspection throughput. The 1100TX and 5500TX devices support the same I/O modules as the 8200TX and 8400TX so these models can support the same capacity on a per-module basis, but they have fewer module slots for a reduced overall performance capacity. The supported standard I/O modules are identified in Section 8.

The vTPS is a virtual appliance supported on VMware and KVM. Each virtual platform supports a virtual serial console and virtual Ethernet management port. Each virtual appliance deployed in normal mode provides 500 Mbps IPS inspection throughput with two vCPUs or 1 Gbps IPS inspection throughput with three vCPUs. When deployed in Performance mode, six vCPUs provide 2 Gbps IPS inspection throughput. The vTPS supports one vNIC (VMware) or one bridge interface (KVM) for management. The concept of I/O modules is not applicable to the vTPS, which has two virtual data ports.

The TOE software incorporates a hardened Linux-4.14.76-yocto-standard operating system. All hardware models include external user disk memory (CFast or SSD) that is used to store all traffic logs, snapshots, ThreatDV URL Reputation Feed, User-defined URL Entries database, and packet capture data. The external memory can also be used for troubleshooting purposes. The vTPS appliance does not have a separate user disk. Instead, it has a single-disk architecture with either an 8-GB user disk partition (for standard) or 16-GB user disk partition (for Performance).

4 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 Final ETR.

4.1 Security Audit

The TOE is able to generate audit records for security relevant events. 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 drops below 25% capacity.

4.2 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 cryptographic key destruction. The cryptographic mechanisms support SSH used for secure communication, both as client and server.

4.3 Identification and Authentication

The TOE requires 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 the local console.

4.4 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 claimed PP. Each user must be assigned a role in order to perform any management action. The TOE provides authorized administrators with a command line interface (CLI), accessible locally via direct console connection and remotely via SSH, for TOE configuration and to monitor, collect, log, and react in real-time to potentially malicious network traffic.

4.5 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.

4.6 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.

4.7 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.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For virtual Network Devices (vNDs), this assumption applies to the physical platform on which the virtual machine (VM) runs.
- The device is assumed to provide networking 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 a computing platform for general purpose applications (unrelated to networking functionality).

  In the case of vNDs, the virtualization system (VS) is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent 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. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes 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 Network 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.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- The Network 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 Network Device are protected by the platform on which they reside.

- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 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 shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
    - *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6])
- This evaluation covers only the specific software distribution and 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) v5.3 Security Target, Version 1.0, 1 January 2022 ([7]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- 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 VR.

6 Documentation

The vendor 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 the TOE is as follows:

- *Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.3*, 1 January 2022 ([8])
- *Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide*, September 2020 ([9])
- *Trend Micro TippingPoint Threat Protection System Command Line Interface Reference*, November 2019 ([10])
- *Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide*, June 2019 ([11]).

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

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 TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

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

- *Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e*, Version 1.0, 31 January 2022 ([14]).

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Trend Micro TippingPoint Threat Protection System (TPS) v5.3*, Version 1.0, 31 January 2022 ([13]).

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 that claims conformance to *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The evaluation team devised a Test Plan based on the Test Activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]). 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, from April 1, 2021 through December 23, 2021.

The evaluators received the TOE in the form that 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* were fulfilled.

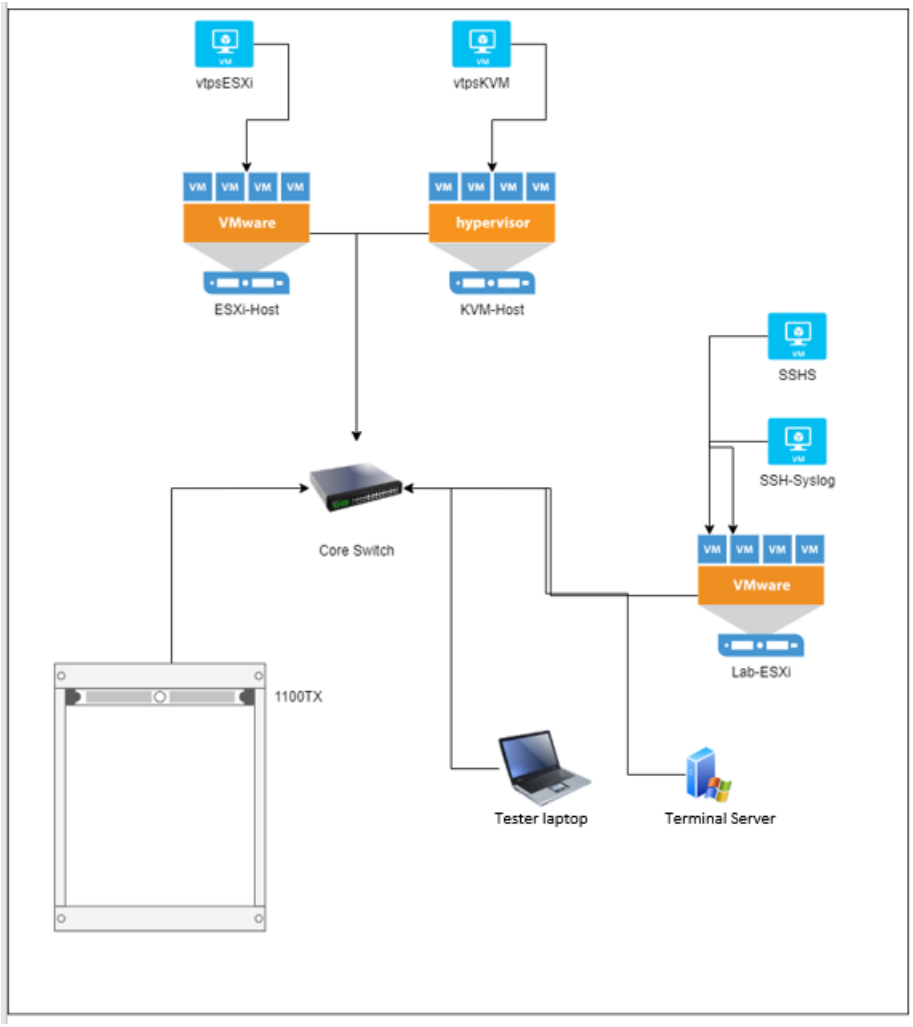
7.1 Test Configuration

The evaluation team established a test configuration including the following TOE instances, all running TPS v5.3.0 software:

- TPS 1100TX appliance
- vTPS running on ESXi 6.5 on Intel Xeon Silver 4116 (Skylake) processor
- vTPS running on KVM 1.5.3 on RHEL 7.5 on Intel Xeon Gold 6126 (Skylake) processor.

The following figure depicts the test environment established for testing the TOE.

Figure 1: TOE Test Configuration



- SSH-Syslog—used as the external audit server. It included the following software:
  - Ubuntu 20.04.3 LTS
  - rsyslog 8.2001.0
  - OpenSSH 8.2p1
  - Wireshark 3.2.3
- Tester laptop—hosts test tools used in vulnerability testing. It included the following software:
  - Kali Linux 2019.4
  - Wireshark 3.0.5
  - Python 2.7
- Terminal Server—provides tester access to test network. It included the following software:
  - Windows Server 2016 1607
  - MobaXterm Professional v12.3
  - PuTTY v0.71
  - Wireshark 3.0.4

- SSHS Server—provided SSH server used to test TOE SSH client functionality. It included the following software:
  - Ubuntu 18.04
  - sshd 7.6p1.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE comprises the following appliances running TPS software v5.3.0:

- TPS 1100TX
- TPS 5500TX
- TPS 8200TX
- TPS 8400TX
- vTPS.

The 1100TX includes one I/O module slot, the 5500TX and the 8200TX include two I/O module slots, and the 8400TX includes four I/O module slots. The following standard I/O modules are supported for the 1100TX, 5500TX, 8200TX, and 8400TX security devices.

Standard I/O Modules	Trend Micro Part Number
TippingPoint 6-Segment Gig-T	TPNN0059
TippingPoint 6-Segment GbE SFP	TPNN0068
TippingPoint 4-Segment 10 GbE SFP+	TPNN0060
TippingPoint 1-Segment 40 GbE QSFP+	TPNN0069

The vTPS virtual appliance consists of TPS v5.3.0, running on hosts with Intel Xeon CPUs based on Ivy Bridge or newer that support the RDRAND instruction and either

- an ESXi Hypervisor: Version 5.5 (Patch 3116895), Version 6.0 (Patch 5572656), Version 6.5, or Version 6.7, or
- a RHEL version 7.1 KVM.

The vTPS virtual appliance uses virtual data ports and does not require I/O modules.

The vTPS appliance is provided as one of the following image files:

- vTPS_vmw_5.3.0_xxxx.zip (standard)
- vTPS_vmw_performance_v5.3.0_xxxx.zip (performance).

Depending on configuration, the TOE in its evaluated configuration may require the following components in its operational environment:

- An SSH-protected syslog server that receives audit events from the TOE
- Workstation or terminal emulator equipped with SSH client software for administrator access to the CLI.

8.2 Excluded Functionality

The following features and capabilities of Trend Micro TippingPoint Threat Protection System (TPS) v5.3 are not covered by the evaluation:

- The Local Security Management (LSM) component of the product provides remote administrative management. The LSM is a GUI accessible over HTTPS. In the evaluated configuration, all management must be performed using the CLI

- The Digital Vaccine service is provided by the TOE developer and assumed to be a trusted service. It may be used in the evaluated configuration, however it is not included in the TOE itself and therefore no claims are made about its ability to provide adequate or timely filter updates
- 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 organization to increase the overall inspection capacity of the TPS by grouping multiple TX Series devices and pooling their resources. Stacking configurations are not included in the evaluated configuration. The devices are being evaluated in a standalone configuration
- Optional bypass I/O modules are available for the 1100TX, 5500TX, 8200TX, and 8400TX security devices that provide high availability for copper and fiber segments. These modules are not included in the TOE and must not be used in the evaluated configuration
- The TPS intrusion prevention services including collection, inspection, analyzation, and reaction capabilities applied to network traffic have not been evaluated and no claims are made in relation to these functions. However, they may be used without affecting the claimed security functionality.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Trend Micro TippingPoint Threat Protection System (TPS) v5.3, Part 2 ([12]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]). The evaluation determined the TOE satisfies the conformance claims made in the Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Security Target, of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence.

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

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

Searches of public vulnerability repositories were performed on 7 July 2021 and again on 12 January 2022.

The evaluation team searched the following public vulnerability repositories:

- National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search)
- US-CERT (http://www.kb.cert.org/vuls/html/search).

The evaluation team used the following search terms in the searches of these repositories:

- trend micro
- tippingpoint
- threat protection system
- tps
- openssl
- linux 4.14
- yocto
- intel pentium d-1517
- intel xeon d-1559
- intel xeon e5-2648lv3
- broadwell
- haswell.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. 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.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed PP. 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

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs 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 TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

The TOE supports three levels of password length: 1, 8, and 15. The validators recommend that the TOE be configured to use the strongest and longest password length whenever possible for the organization, and note that lowest level of password provides no real protection (although it is permitted by the SFRs).

11 Security Target

The ST for this product's evaluation is *Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Security Target*, Version 1.0, 1 January 2022 ([7]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
cPP	collaborative Protection Profile
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IT	Information Technology
KVM	Kernel-based Virtual Machine
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TPS	Threat Protection System
TSF	TOE Security Functions
TSS	TOE Summary Specification
VM	Virtual Machine
vND	virtual Network Device
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019.

[7] Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Security Target, Version 1.0, 1 January 2022.

[8] Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.3, Version 1.0, 1 January 2022.

[9] Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, September 2020.

[10] Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, November 2019.

[11] Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, June 2019.

[12] Evaluation Technical Report for Trend Micro TippingPoint Threat Protection System (TPS) v5.3, Part 2 (Leidos Proprietary), Version 1.0, 31 January 2022.

[13] Assurance Activities Report for Trend Micro TippingPoint Threat Protection System (TPS) v5.3, Version 1.0, 31 January 2022.

[14] Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.0, 31 January 2022.