MINISTRY OF DIGITAL

# C140 Certification Report

## Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0

File name: ISCB-3-RPT-C140-CR-v1
Version: v1
Date of document: 9 June 2025
Document classification : PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
200601006881 (726630-U)
www.cybersecurity.my

Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
T +603 8800 7999 F +603 8008 7000 H 1 300 88 2999

SECURING
OUR
CYBERSPACE

# C140 Certification Report

## Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0

9 June 2025

ISCB Department

**CyberSecurity Malaysia**

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999  Fax: +603 8008 7000
http://www.cybersecurity.my

# Document Authorisation

| | |
|---|---|
| ***DOCUMENT TITLE:*** | C140 Certification Report |
| ***DOCUMENT REFERENCE:*** | ISCB-3-RPT-C140-CR-v1 |
| ***ISSUE:*** | v1 |
| ***DATE:*** | 9 June 2025 |
| ***DISTRIBUTION:*** | UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION |

# Copyright Statement

Registered office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 200601006881 (726630-U)

*Printed in Malaysia*

# Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) https://iscb.cybersecurity.my/index.php/certification/product-certification/mycc/ and the Common Criteria Recognition Arrangement at http://www.commoncriteriaportal.org

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

# Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, Version 2022 Revision 1 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, Version 2022 Revision 1 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# Document Change Log

| RELEASE | DATE | PAGES AFFECTED | REMARKS/CHANGE REFERENCE |
|---|---|---|---|
| d1 | 5 June 2025 | All | Initial draft |
| v1 | 9 June 2025 | All | Final version of the document. |

# Executive Summary

The Target of Evaluation (TOE) is Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0. The TOE is a network security platform that offers threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks.

The scope of the evaluation is defined by the Security Target ([6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Securelytics Security Evaluation Facility (SEF) and the evaluation was completed on 2 May 2025.

This certification report is associated with the product evaluation certificate issued on 16 June 2025 and the Security Target (Ref [6]). The certification will expire five (5) years from the date of certificate issuance.

It is the responsibility of the user to ensure that Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0 meets their requirements. It is recommended that potential users of the TOE refer to the Security Target ([6]) and this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

# Index of Tables

# Index of Figures

# 1 Target of Evaluation

## 1.1 TOE Description

1 The TippingPoint Threat Protection System v6.4.0 is a network device provided as a standalone hardware or virtual appliance. The appliances include the TPS v6.4.0 software.

2 Each appliance also includes the hardened Linux-5.4.58-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 TPS version 6.4.0 appliances included in the evaluation are the physical devices TPS 1100TX, TPS 5500TX, TPS 8200TX, TPS 8400TX, TPS 8600TXE, TPS 9200TXE, and the virtual vTPS device. vTPS appliances do not have a separate user disk. The vTPS virtual appliances have a single-disk architecture with either an 8-GB user disk partition (for standard) or 16-GB user disk partition (for Performance). The TX hardware models include 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, 8200TX, 8600TXE, and 9200TXE include two I/O module slots, and the 8400TX includes four I/O module slots. The supported standard I/O modules are identified in Section 1.1. The concept of I/O modules is not applicable to vTPS which has two virtual data ports

3 The TOE provides intrusion prevention services including monitoring, collection, inspection, analyzation, and reaction capabilities applied to network traffic in real-time. The TOE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination. The TOE provides administrators with a CLI accessible via SSH to manage the TOE and its IPS functions and to monitor, collect, log, and react in real-time to potentially malicious network traffic. Evaluation of the IPS services focuses on inspecting the IPv4 and IPv6 traffic (TCP, UDP, ICMP, etc.).

4 The TOE requires users to be identified and authenticated before they can access any of the TOE functions. For each session, the user is required to log in prior to successfully establishing a session through which TOE functions can be exercised. The only capabilities allowed prior to users authenticating are the display of the warning

banner before authentication, and the TOE may send Echo Reply in response to Echo Request ICMP messages received at the Management interface. The banner is displayed on every login attempt.

5 The administrators interact locally with the TOE via console or remotely using SSH where OpenSSL is used to implement SSH and its underlying core cryptographic algorithms to secure the underlying communications. The TOE also uses SSH for communications with trusted external syslog servers. The TOE is operated in FIPS mode and includes NIST validated cryptographic algorithms.

6 The TOE local and remote administration is provided through the Command Line Interface (CLI). The TOE supports Super User, Admin, and Operator roles that collectively represent the Administrator role described in the Security Problem Definition and the Security Functional Requirements. Each user must be assigned a role in order to perform any management action.

7 The TOE can communicate with the Trend Micro website to download TOE updates. The management CLI provided by the TOE can be used by Super User or Administrator, administrators to update the TOE, and to query the currently executing software version of the TOE. Software updates are available as package files. The update package is published on the Trend Micro support website and protected with a SHA-256 hash and signed using 2048-bit RSA public/private key pair.

8 The TOE audit log provides an internal log implementation that can be used to store and review audit records locally. Access is available to the Super User. The TOE can also be configured to send generated audit records to an external Syslog server using SSH. When configured to send audit records to a syslog server, audit records are written to the external syslog as they are written locally to the TOE Audit log.

9 The TSF includes the following security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels
- Intrusion Prevention System

## 1.2 TOE Identification

10 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

| | |
|---|---|
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Project Identifier** | C140 |
| **TOE Name** | Trend Micro TippingPoint Threat Protection System (TPS) |
| **TOE Version** | v6.4.0 |
| **Security Target Title** | Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0 Security Target |
| **Security Target Version** | 1.0 |
| **Security Target Date** | 24 April 2025 |
| **Assurance Level** | Evaluation Assurance Level 2 |
| **Criteria** | Common Criteria for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref [2]) |
| **Methodology** | Common Methodology for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref [3]) |
| **Protection Profile Conformance** | None |
| **Common Criteria Conformance** | CC Part 2 Extended<br>CC Part 3 Conformant |
| **Sponsor** | Leidos Inc<br>6841 Benjamin Franklin Dr, Columbia, MD 21046, USA |
| **Developer** | Trend Micro Inc<br>11305 Alterra Parkway<br>Austin, TX 78758, USA |
| **Evaluation Facility** | Securelytics SEF<br>A-19-06, Tower A, Atria SOFO Suites, Jalan SS 22/23. Damansara Utama, 47400 Petaling jaya, Selangor, Malaysia |

## 1.3 Security Policy

11 Organisational Security Policies (OSPs) are used to provide a basis for security objectives that are commonly desired by TOE Owners in this operational environment,

but for which it is not practical to universally define the assets being protected or the threats to those assets.

12 OSPs for the TOE as described in the Security Target (Ref [6]):

Table 2: Organizational Security Policies

| Assumption | Statements |
|---|---|
| P.ACCESS_BANNER | The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. |
| P.ANALYZE | Analytical processes and information to derive conclusions about potential intrusions must be applied to IPS data and appropriate response actions taken. |

## 1.4 TOE Architecture

13 The TOE includes both physical and logical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

### 1.4.1 Logical Boundaries

14 The TOE consists of security functions provided by the TOE that are identified in the Security Target ([6]).

Table 3: TOE Logical Boundaries

| | |
|---|---|
| Security Audit | The TOE can generate audit records for security relevant events, including IPS related 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 remaining space available for storage of local audit records drops below 25% capacity. |
| 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 |
| 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.<br>The TOE supports the local (i.e., on device) definition of administrators with usernames and either passwords or public keys. 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 minimum password length is configurable based on administrative configuration.<br>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. |
| 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 Administrator role. Each user must be assigned a role to perform any management action. The TOE provides administrators with a CLI accessible via SSH or locally through the console interface for TOE configuration and to monitor, collect, log, and react in real-time to potentially malicious network traffic. |
| 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.<br>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.<br>The TOE performs tests for software module integrity and cryptographic known-answer tests. |
| 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.<br>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). |

| | |
|---|---|
| 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.<br>The TOE also uses SSH to protect the transmission of audit records to an external audit server. |
| Intrusion Prevention System | The TOE provides intrusion prevention services including collection, inspection, analyzation, and reaction capabilities applied to network traffic in real-time. |

### 1.4.2 Physical Boundaries

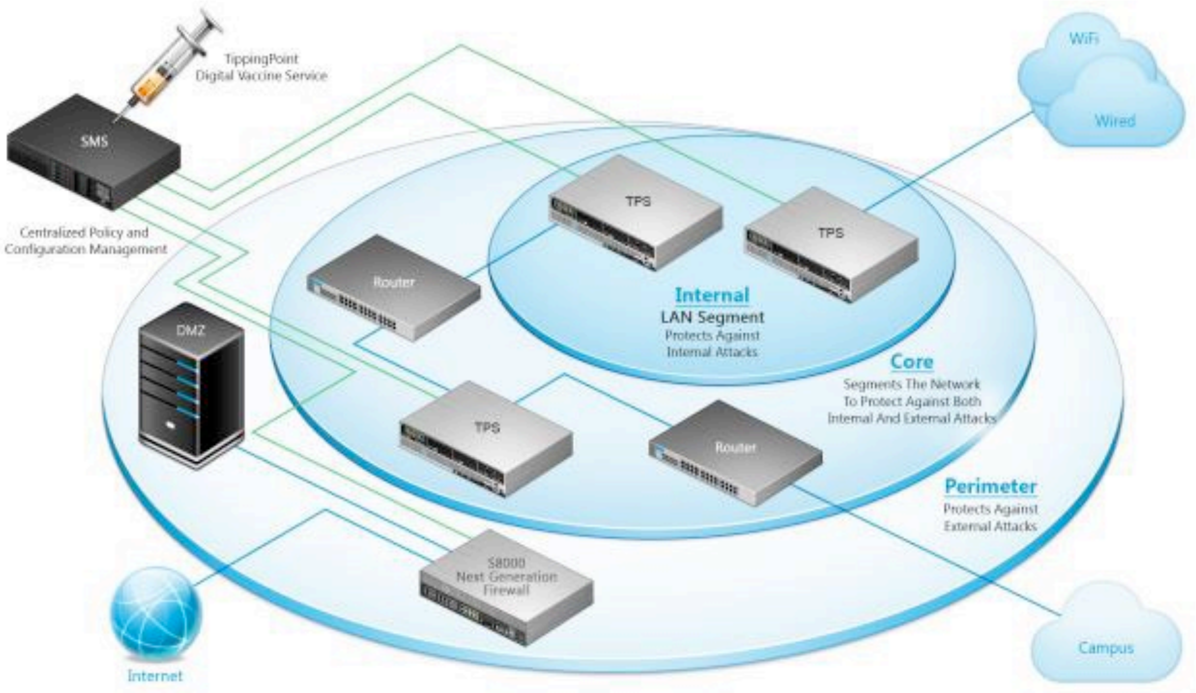

Figure 1: Sample TPS Network Deployment Scenario

15 The TOE is a self-contained hardware appliance or VM with TPS v6.4.0 software.

16 The following table identifies the hardware appliance models included in the TOE.

Table 4: TOE Hardware Appliances

| Device | Main Processor | Storage | Network Ports | Operating System / Software |
|---|---|---|---|---|
| TPS 1100TX | Intel Pentium D-1517 (Broadwell) CPU / 4 Cores, 8 Threads, 1.6GHz, 25W TDP | Storage = 8GB CFAST (Internal) / 8GB (External) | One I/O Module Slot Hot-Swappable<br>Up to 6 1GE Segments, Up to 4 10GE Segments, 1 40GE Segment | Linux-5.4.58-yocto-standard<br>OpenSSL 3.0.9 |
| TPS 5500TX | Intel Xeon D-1559 (Broadwell) CPU / 12 Cores, 24 Threads, 1.5GHz, 45W TDP | Storage = 32GB CFAST (Internal) / 32GB (External) | Two I/O Module Slots, Hot-Swappable<br>Up to 12 1GE Segments, Up to 8 10GE Segments, Up to 2 40GE Segments | Linux-5.4.58-yocto-standard<br>OpenSSL 3.0.9 |
| TPS 8200TX | 2x Intel Xeon E5-2648Lv3 (Haswell) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W TDP | Storage = 32GB CFAST (Internal) / 32GB (External) | Two I/O Module Slots, Hot-Swappable<br>Up to 12 1GE Segments, Up to 8 10GE Segments, Up to 2 40GE Segments | Linux-5.4.58-yocto-standard<br>OpenSSL 3.0.9 |
| TPS 8400TX | 2x Intel Xeon E5-2648Lv3 (Haswell) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W TDP | Storage = 128 GB DRAM (Internal) / 32 GB (External) | Four I/O Module Slots, Hot-Swappable<br>Up to 24 1GE Segments, Up to 16 10GE Segments, Up to 4 40GE Segments | Linux-5.4.58-yocto-standard<br>OpenSSL 3.0.9 |
| TPS 8600TXE | 2x Intel Xeon Gold 5318N (Ice Lake) - 80 Cores @ 2.0GHz | Storage = 32GB CFAST (Internal) / 240GB | Two I/O Module Slots, Hot-Swappable<br>Up to 12 25GE/10GE/1GE | Linux-5.4.58-yocto-standard |

| Device | Main Processor | Storage | Network Ports | Operating System / Software |
|---|---|---|---|---|
| | | NVMe SSD (External) | Segments, Up to 8 100GE/40GE Segments | OpenSSL 3.0.9 |
| TPS 9200TXE | 2x Intel Xeon Gold 5318N (Ice Lake) - 80 Cores @ 2.0GHz | Storage = 32GB CFAST (Internal) / 240GB NVMe SSD (External) | Two I/O Module Slots, Hot-Swappable<br>Up to 12 25GE/10GE/1GE Segments, Up to 8 100GE/40GE Segments | Linux-5.4.58-yocto-standard<br>OpenSSL 3.0.9 |

17 The TippingPoint vTPS is deployed between layer 2 (L2) broadcast domains (virtual switches) using an image with either “Normal” or “Performance” options. Performance option offers an increased capacity for vCPUs and threading.

18 Virtual Machine appliance TOEs consist of TPS v6.4.0, including Linux-5.4.58-yocto-standard and OpenSSL 3.0.9 and requires the following:

Table 5: TOE Virtual Machine Appliances

| Device | Image | Number of vCPUs | Memory | Disk | Operating System / Software |
|---|---|---|---|---|---|
| vTPS | Normal Option:<br>VMware: vTPS_vmw_6.4.0_xxxx.zip<br>Or<br>KVM:<br>vTPS_kvm_6.4.0_xxxx.tar.gz | 2 – 3 | 8GB | 16.2GB | ESXi Hypervisor version: Version 7.0 or 8.0 (only paid versions supported)<br>or<br>RHEL version 8 or 9 KVM |
| | Performance Option:<br>VMware: vTPS_vmw_6.4.0_xxxx.zip<br>Or<br>KVM: | 6 | 16GB | 16.2GB | ESXi Hypervisor version: Version 7.0 or 8.0 (only paid versions supported) |

| Device | Image | Number of vCPUs | Memory | Disk | Operating System / Software |
|---|---|---|---|---|---|
| | vTPS_kvm_6.4.0_xxxx.tar.gz | | | | or<br>RHEL version 8 or 9 KVM |

19 The TippingPoint vTPS is deployed between layer 2 (L2) broadcast domains (virtual switches). The virtual appliances are supported on hosts with Intel Xeon CPUs based on Broadwell or newer that support the RDSEED instruction.

20 The TOE virtual (VM) appliances are delivered as an installation disk (or ISO image). They require that one of the following are installed on the host hardware system:

- VMware ESXi 7.0 or 8.0 or
- RHEL version 8 or version 9 KVM

21 Additional hardware Requirements:

- External audit storage requires the use of syslog servers.
- An administrative workstation or terminal emulator equipped with SSH client software.

### 1.4.3 Exclusions

22 The TippingPoint Threat Protection System solution includes Local Security Management (LSM) and Security Management System (SMS) components that provides remote administrative management. In the evaluated configuration, all management must be performed using the CLI.

23 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.

24 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 excluded from the evaluated configuration and must not be configured or used.

25 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 configurations are not covered in the scope of the evaluation.

26 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 or TXE Series devices and pooling their resources. Stacking configurations are not included in the evaluated configuration. The devices are being evaluated in a standalone configuration.

27 Optional bypass I/O modules are available for the physical TOE devices that provide HA for copper and fiber segments. These modules are not included in the TOE and must not be used in the evaluated configuration.

## 1.5 Clarification of Scope

28 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

29 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

30 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

## 1.6 Assumptions

31 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

### 1.6.1 Operational Environment Assumptions

32 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 6: Assumptions for the TOE environment

| Assumption | Statements |
|---|---|
| A.ADMIN_CREDENTIALS_SECURE | The administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside. |

| Assumption | Statements |
|---|---|
| A.CONNECTIONS | It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks. |
| A.LIMITED_FUNCTIONALITY | 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 computing platform for general purpose applications (unrelated to networking functionality). |
| A.PHYSICAL_PROTECTION | The network 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.<br>This protection is assumed to be sufficient to protect the device and the data it contains. |
| A.TRUSTED_ADMIISTRATOR | The 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 being appropriately trained, following policy, and adhering to guidance documentation.<br>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. |
| A. REGULAR_UPDATES | The network device firmware and software are assumed to be updated by an administrator on a |

| Assumption | Statements |
|---|---|
|  | regular basis in response to the release of product updates due to known vulnerabilities. |

## 1.7 Evaluated Configuration

33 To achieve full compliance with the evaluated Common Criteria certification, specific features must be configured precisely, and devices must operate within designated guidelines. Additionally, some features fall outside the scope of this evaluation.

34 Ensuring the TPS device is configured within the requirements of the evaluated configuration for Common Criteria requires the following configuration actions:

- The TPS must be configured to support the Federal Information Processing Standards 140-2 (FIPS 140-2) cryptographic requirements. The fips-mode-enable command enables the Federal Information Processing Standard (FIPS) on a TPS device.
- Before run this command, always reset the device to factory default settings. When run this command, it prompts you to confirm that you want to enable FIPS mode. After enable FIPS mode, it cannot be disabled except by resetting the device to factory defaults. After run this command, you must reboot the device to enable FIPS mode. Use the show fipsmode command to verify FIPS mode is enabled. FIPS Mode restricts the cryptographic mechanisms to FIPS-approved algorithms.
- During initial device configuration an administrative account is created with the default Super User role. The Super User role gives the account full access to the device. This administrative account is used to complete initial configuration. The password must be set prior to first use by the administrator performing the initial setup; there is no ‘default’ password that can be used to access the TOE. The Super User account itself must also be used to create other users and associate roles with roles. Other than super user, the default roles are: administrator and operator.
- The Trend Micro TPS and vTPS appliances must be deployed in a physically secure location to prevent physical tampering. Any person with physical access to the device must have the same level of trustworthiness as an authorized administrator.
- To manage a Trend Micro TPS and vTPS device in a way consistent with the evaluated configuration, device management must be performed via the CLI. Administrators manage the TOE remotely using an SSH connection to the Ethernet Management

port on the TOE appliance or locally through the console interface or locally through a direct connection to the Ethernet Management port. Each method provides access to the CLI after an administrator successfully logs in. Prior to administrative login, the Management interface will respond to ICMP requests to confirm connectivity (for remote administrative connections) and displays a warning banner for both local and remote connections. No other TSF-mediated actions are permitted on behalf of an administrative user until the user is successfully authenticated. SSH access is enabled by default to allow CLI access to the device. No configuration is necessary. Non-secure access through Telnet is not permitted.

- In order to log in, the user must provide an identity and authentication data that matches an identity configured on the TOE. Users are defined locally within the TOE with a user identity, password, and user role. Administrators accessing the Ethernet Management port can be defined with an SSH public key for public key-based authentication for SSH connections rather than a password. To upload a public SSH key see CLI SSH Configuration Section “To upload a user public key”. Users are authenticated directly by the TOE. Any resulting session is dependent upon successful authentication and established sessions are associated with the role(s). SSH access is enabled by default to allow CLI access to the device. While the TOE is configured out-of-the-box to be running an SSH server, it does not supply a client to access it, so users are free to use a third-party SSH client of their choosing to connect to the TOE's IP address over port 22.
- Telnet, and HTTP, and connections over untrusted networks are not supported and must not be enabled.

35 The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST (Ref.[6]). In particular, the SSH protocol implemented by the Trend Micro TippingPoint devices have been tested, and only to the extent specified by the security functional requirements. The following protocols and features identified in ST (Ref. [1]) have not been included in the evaluated configuration:

TOE:

- The TippingPoint Threat Protection System solution includes Local Security Management (LSM) and Security Management System (SMS) components that provides remote administrative management. 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 excluded from the evaluated configuration and must not be configured or used.
- 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 configurations are not covered in the scope of the evaluation.
- 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 or TXE 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 physical 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.

## 1.8 Delivery Procedures

36 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

37 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

### 1.8.1 TOE Delivery

#### 1.8.1.1 Hardware Delivery

38 Once a hardware appliance instance of the TOE is manufactured, it is securely packaged. Packaging tape is used to seal the packages containing the TOE hardware appliance and associated accessory kit. The manufacturing facility (Benchmark Phoenix) sends the packaged TOE appliance to Trend's Distribution Center (DB Schenker Dallas). The Trend Distribution Center holds the packaged TOE appliances in a secure area before an order is shipped to prevent tampering. When an order for the TOE is received, the Trend Distribution Center uses a private distribution service (e.g., UPS) to distribute the package to the customer. On every TOE chassis, a security label has been affixed to ensure that the chassis is not tampered with. If the unit is opened, then the label is broken, indicating the unit may have been tampered with and all warranties are void.

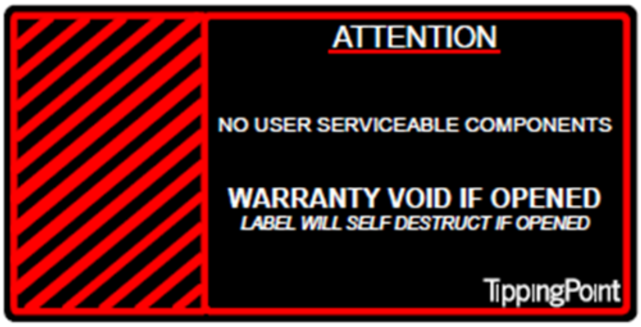
ATTENTION
NO USER SERVICEABLE COMPONENTS
WARRANTY VOID IF OPENED
LABEL WILL SELF DESTRUCT IF OPENED
TippingPoint

Figure 2: Example of Cover Security/Warranty Void Label

#### 1.8.1.2 Software Delivery

39 As part of the delivery process, TOE software updates are posted on the Threat Management Center (TMC) website (https://tmc.tippingpoint.com). This site requires authentication via the customer assigned credentials. The download and update process is as follows:

- TOE "packages" are downloaded from TMC via a TLS connection. The package files are encrypted. A public/private key system (RSA 2048) is used for encryption.
- When the package is loaded onto the device, the package is decrypted and the package is unpacked, provided the keys match. If the decryption fails, log entries are generated indicating there was a problem with the package.
- After the software updates, a reboot is needed. At this point, an MD5 checksum occurs to ensure the package is not corrupt.

- For Digital Vaccine (DV) updates, the MD5 checksum occurs during the installation of the DV (reboots are not needed for DVs).

40 When product updates are released, a release e-mail is sent out to customers to notify them of the update availability.

41 TPS virtual appliance (vTPS) images are made available on TMC. These are downloaded by the customer via a TLS connection. The image itself is signed using Trend Micro certificate. The customers install the image into their own server hardware running supported hypervisors.

# 2 Evaluation

43 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2022 Revision 1 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 2022 Revision 1 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

## 2.1 Evaluation Analysis Activities

44 The evaluation activities involved a structured evaluation of the TOE, including the following components:

### 2.1.1 Life-cycle support

45 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

46 The evaluators confirmed that the configuration list includes TOE itself, the parts that comprise the TOE the evaluation evidence required by the SARs in the the Security Target (Ref [6]).

47 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

### 2.1.2 Development

Architecture

48 The evaluators examined the security architecture description (contained in Section 4) and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

49 The security architecture description describes the security domains maintained by the TSF.

50 The initialisation process described in the security architecture description preserves security.

51 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Functional Specification

52 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

53 The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

54 The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

TOE Design Specification

55 The evaluators examined the TOE design (contained in **Error! Reference source not found.**) and determined that the structure of the entire TOE is described in terms of subsystems.

56 The evaluators also determined that all subsystems of the TSF are identified.

57 The evaluators determined that interactions between the subsystems of the TSF were described.

58 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

59 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

60 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

61 The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

### 2.1.3 Guidance documents

62 The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

63 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

64 The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

65 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

66 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

67 The documents for TOE users to refer as guidance are as per listed:

- Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0 Common Criteria Evaluated Configuration Guide (CCECG), v1.0, April 24, 2025.
- Trend Micro TippingPoint (TPS) Command Line Interface Reference (CLI), December 2024.
- Trend Micro TippingPoint (TPS) Hardware Specification and Installation Guide, December 2024.

- Trend Micro TippingPoint (TPS) Virtual Threat Protection System (vTPS) User Guide, April 2024.

### 2.1.4 IT Product Testing

68 Testing at EAL2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

#### 2.1.4.1 Assessment of Developer Tests

69 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidence submitted.

#### 2.1.4.2 Independent Functional Testing

70 At EAL2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

71 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 7: Independent Functional Test

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| F001 – Identification and Authentication<br>FIA_AFL.1<br>FIA_PMG_EXT.1<br>FIA_UAU.1 | • To verify that the TOE able to detect when within 1 to 10 unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using an | Passed. Result as expected. |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| FIA_UAU.5<br>FIA_UAU.7<br>FIA_UID.1 | administrator configurable positive integer password.<br>• To verify that the TOE able to provide password management capabilities for administrative password.<br>• To verify that the TOE able to display of the warning banner in accordance with FTA_TAB.1 and send Echo Reply in response to Echo Request ICMP messages received at the Management interface on behalf of the user to be performed before the user is authenticated.<br>• To verify that the TOE able to require each administrative user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.<br>• To verify that the TOE able to provide password-based authentication, SSH public-key based authentication to support user authentication and able to authenticate any user's claimed identity according to the locally configured authentication mechanism.<br>• To verify that the TOE able to provide obscured feedback to the administrative user while the authentication is in progress. | |
| F002 – Security Management and User Data Protection | • To verify that the TOE able to restrict the ability to enable the functions to perform manual updates to Administrators. | Passed. Result as expected. |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| FMT_MOF.1/ ManualUpdate<br>FMT_MOF.1/ Functions<br>FMT_MTD.1<br>FMT_SMF.1/Core<br>FMT_SMF.1/IPS<br>FMT_SMR.2 | • To verify that the TOE able to restrict the ability to determine the behaviour of; modify the behaviour of the function's transmission of audit data to an external IT entity to Administrators.<br>• To verify that the TOE able to restrict the ability to modify the any TSF data to Administrators.<br>• To verify that the TOE capable of performing the management function meets FMT_SMF.1.1/Core requirements.<br>• To verify that the TOE capable of performing the IPS management function meets FMT_SMF.1/IPS requirements.<br>• To verify that the TOE able to shall maintain the roles, associate users with roles and ensure that the Administrator role shall be able to administer the TOE locally and remotely. | |
| F003 – Security Audit<br>FAU_GEN.1/Audit<br>FAU_GEN.1/IPS<br>FAU_GEN.2<br>FAU_STG.1<br>FAU_STG.2<br>FAU_STG.5 | • To verify that the TOE able to generate record within each audit record and IPS records for the auditable events.<br>• To verify that the TOE able to associate each auditable event with the identity of the user that caused the event.<br>• To verify that the TOE able to store generated audit data. | Passed. Result as expected. |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | • To verify that the TOE able to protect the stored audit data in the audit trail from unauthorized deletion and able to prevent unauthorized modifications to the stored audit data in the audit trail.<br>• To verify that the TOE able to overwrite the oldest stored audit records, generate a warning when audit storage used exceeds 75% of the available storage space if the audit data storage is full. | |
| F004 – Cryptographic Support and Trusted Path<br>FCS_CKM.1<br>FCS_CKM.3<br>FCS_CKM.5<br>FCS_CKM.6/Volatile<br>FCS_CKM.6/Non Volatile<br>FCS_COP.1/Data Encryption<br>FCS_COP.1/Sig<br>FCS_COP.1/Hash<br>FCS_COP.1/KeyedHash<br>FCS_RBG.1<br>FCS_RBG.3<br>FCS_SHC_EXT.1<br>FCS_SHS_EXT.1 | • To verify that the TOE able to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm.<br>• To verify that the TOE able to perform RSA Private Key access, ECC Private Key access, FFC Private value access in accordance with a specified cryptographic key access method TSF internal access only.<br>• To verify that the TOE able to derive cryptographic keys.<br>• To verify that the TOE able to destroy cryptographic keys SSH session keys (e.g. AES Keys, HMAC keys), CTR_DRBG key, SSH-RSA peer public key, SSH-ECC peer public key stored in volatile storage when no longer needed and able to destroy cryptographic kyes and keying material specified by FCS_CKM.6.1 in | Passed. Result as expected. |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| FTP_ITC.1<br>FTP_TRP.1 | accordance with a specified cryptographic key destruction method.<br>• To verify that the TOE able to destroy cryptographic keys SSH-RSA local Private Keys, SSH Peer public keys, SSH user keys stored in non-volatile storage when directed to by an administrator and able to destroy cryptographic kyes and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method key zeroization.<br>• To verify that the TOE able to perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in CBC, GCM modes] and cryptographic key sizes 128 bits, 256 bits.<br>• To verify that the TOE able to perform cryptographic signature services generation and verification in accordance with a specified cryptographic algorithm and cryptographic key sizes.<br>• To verify that the TOE able to perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512 and cryptographic key sizes message digest sizes 160, 256, 384, 512 bits. | |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | • To verify that the TOE able to perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 and cryptographic key sizes 160, 256, 512 bits and message digest sizes 160, 256, 512 bits.<br>• To verify that the TOE able to perform deterministic random bit generation services using CTR_DRBG (AES) in accordance with ISO/IEC 18031:2011 after initialization with a seed, use a platform-based noise source for initialized seeding and update the RBG state by reseeding using a the TSF hardware-based noise source RDSEED.<br>• To verify that the TOE able to seed the RBG using TSF hardware-based noise source RDSEED with a minimum of 256 bits of min-entropy.<br>• To verify that the TOE able to shall implement the SSH protocol in accordance with: RFC(s) 4251, 4252, 4253, 4254, [5647, 5656, 6668].<br>• To verify that the TOE able to ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [no other method]. | |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | • To verify that the TOE able to ensure that, as described in RFC 4253, packets greater than [256K] bytes in an SSH transport connection are dropped.<br>• To verify that the TOE able to ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com.<br>• To verify that the TOE able to ensure that the SSH public-key based authentication implementation uses [ssh-rsa, ecdsasha2nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521] as its public key algorithm(s) and rejects all other public key algorithms.<br>• To verify that the TOE able to ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512, implicit] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).<br>• To verify that the TOE able to ensure that [diffie-hellman-group14-sha1, ecdhsha2-nistp256] ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol. | |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | • To verify that the TOE able to ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.<br>• To verify that the TOE able to ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and no other methods as described in RFC 4251.<br>• To verify that the TOE able to implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [5647, 5656, 6668, 8268].<br>• To verify that the TOE able to ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [password-based].<br>• To verify that the TOE able to ensure that the SSH public-key based authentication implementation uses [ssh-rsa] as its public key algorithm(s) and rejects all other public key algorithms. | |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | • To verify that the TOE able to ensure that diffie-hellman-group16-sha512, diffie-hellmangroup18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.<br>• To verify that the TOE able to ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed. | |
| F005 – TSF Protection<br>FPT_APW_EXT.1<br>FPT_FLS.1<br>FPT_SKP_EXT.1<br>FPT_STM.1<br>FPT_STM.2<br>FPT_TST.1<br>FPT_TUD_EXT.1 | • To test that the TOE able to store administrative passwords in non-plaintext form and prevent the reading of plaintext administrative passwords.<br>• To test that the TOE able to preserve a secure state when the following types of failures occur.<br>• To test that the TOE able to prevent reading of all pre-shared keys, symmetric key, and private keys.<br>• To test that the TOE able to provide reliable time stamps.<br>• To test that the TOE able to allow the Administrator to set the time, configure another time source.<br>• To test that the TOE able to run a suite of the self-tests during initial | Passed. Result as expected. |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | start-up to demonstrate the correct operation of the TSF and able to provide authorized users with the capability to verify the integrity of TSF data and the TSF.<br>• To test that the TOE able to provide Administrators the ability to query the currently executing version of the TOE firmware/software and no other TOE firmware/software version, provide Administrators the ability to manually initiate updates to TOE firmware/software and no other update mechanism and provide means to authenticate firmware/software updates to the TOE using a digital signature prior to installing those updates. | |
| F006 – TOE Access<br>FTA_SSL.3<br>FTA_SSL.4<br>FTA_TAB.1 | • To test that the TOE able to terminate an interactive session(s) after an administrator configured inactivity time interval from 1 to 180 minutes.<br>• To test that TOE able to allow user initiated termination of the user's own interactive session.<br>• To test that the TOE can display an Administrator-specified advisory warning message regarding unauthorized use of the TOE message. | Passed. Result as expected. |
| F007 – Intrusion Prevention System<br>IPS_ABD_EXT.1 | • To test that the TOE able to support the definition of anomaly activity. | Passed. Result as expected. |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| IPS_NTA_EXT.1<br>IPS_SBD_EXT.1 | • To test that the TOE able to allow the operations to be associated with anomaly-based IPS policies.<br>• To test that the TOE able to perform analysis of IP-based network traffic forwarded to the TOE's sensor interfaces and detect violations of administratively-defined IPS policies.<br>• To test that the TOE able to allow the signatures to be assigned to sensor interfaces configured for promiscuous mode, and to interfaces configured for inline mode, and support designation of one or more interfaces as 'management' for communication between the TOE and external entities without simultaneously being sensor interfaces.<br>• To test that the TOE support inspection of packet header contents and be able to inspect at least the requirements.<br>• To test that the TOE able to support inspection of packet payload data and be able to inspect at least the data elements to perform string-based pattern-matching.<br>• To test that the TOE able to detect the following header-based signatures using fields identified in IPS_SBD_EXT.1.1 at IPS sensor interfaces. | |

| TEST ID | DESCRIPTIONS | RESULTS |
|---|---|---|
| | • To test that the TOE able to detect all the traffic-pattern detection signatures, and to have signatures applied to IPS sensor interfaces.<br>• To test that the TOE able to allow the operations to be associated with signature-based IPS policies requirements and support stream reassembly or equivalent to detect malicious payload even if it is split across multiple non-fragmented packets. | |

72 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration testing

73 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

74 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation

75 The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) www.google.com

b) www.yahoo.com

c) www.bing.com

d) www.cve.org

76 The penetration tests focused on:

a) Connectivity Check;

b) Traceroute IP;

c) Port Scanning;

d) Banner Grabbing;

e) Packet Crafting;

f) Vulnerability Dependency Check;

g) UDP Flooding Attack;

h) Brite-Force Attack

i) Information leakage via unencrypted network traffic; and

j) Denial of Service.

77 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 4 of the Security Target (Ref [6].

#### 2.1.4.4 Testing Results

78 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

# 3 Result of the Evaluation

79 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7], the Malaysian Common Criteria Certification Body certifies the evaluation of Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0 performed by Securelytics SEF.

80 Securelytics SEF found that Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0 upholds the claims made in the Security Target (Ref [6] and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

81 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

## 3.1 Assurance Level Information

82 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

83 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

84 EAL2 also provides assurance through use of a configuration management system, the secure delivery procedures, and evidence of flaw remediation procedures.

## 3.2 Recommendation

85 The Malaysian Certification Body (MyCB) is strongly recommends that:

a) The users should make themselves familiar with the develop guidance provided with the TOE and pay attention to all security warnings.

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

(*Disclaimer: Opinion and interpretations expressed herein are outside the scope of accreditation*)

# Annex A References

## A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.

[3] The Common Methodology for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.

[4] MyCC Scheme Requirement (MYCC_REQ), v2, CyberSecurity Malaysia, April 2025.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v4, April 2025.

[6] Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0 Security Target, Version 1.0, 24 April 2025.

[7] Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0, Evaluation Technical Report, Version 1.0, 19 May 2025.

## A.2 Terminology

### A.2.1 Acronyms

Table 8: List of Acronyms

| Acronym | Expanded Term |
|---|---|
| CB | Certification Body |
| CC | Common Criteria (ISO/IEC15408) |
| CEM | Common Evaluation Methodology (ISO/IEC 18045) |
| CCRA | Common Criteria Recognition Arrangement |
| IEC | International Electrotechnical Commission |
| ISO | International Organisation for Standardization |
| ISCB | Information Security Certification Body |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |
| MySEF | Malaysian Security Evaluation Facility |
| PP | Protection Profile |
| ST | Security Target |

| Acronym | Expanded Term |
|---|---|
| TOE | Target of Evaluation |

## A.2.2 Glossary of Terms

Table 9: Glossary of Terms

| Term | Definition and Source |
|---|---|
| CC International Interpretation | An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants. |
| Certificate | The official representation from the CB of the certification of a specific version of a product to the Common Criteria. |
| Certification Body | An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA |
| Consumer | The organisation that uses the certified product within their infrastructure. |
| Developer | The organisation that develops the product submitted for CC evaluation and certification. |
| Evaluation | The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC 17065 |
| Evaluation and Certification Scheme | The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA. |
| Interpretation | Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**. |
| Certifier | The certifier responsible for managing a specific certification task. |
| Evaluator | The evaluator responsible for managing the technical aspects of a specific evaluation task. |
| Maintenance Certificate | The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme. |
| National Interpretation | An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only. |

| Term | Definition and Source |
|---|---|
| Security Evaluation Facility | An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy |
| Sponsor | The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer. |

--- END OF DOCUMENT ---