MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

C128 Certification Report

Trend Micro TippingPoint Threat Protection System (TPS) v5.5

File name: ISCB-5-RPT-C128-CR-v1a
Version: v1a
Date of document: 6 July 2023
Document classification : PUBLIC

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

C128 Certification Report

Trend Micro TippingPoint Threat Protection System (TPS) v5.5

6 July 2023

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:	C128 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C128-CR-v1a
ISSUE:	v1a
DATE:	6 July 2023
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. 201601006881 (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.

This certification report is associated with the certificate of product evaluation dated 23 June 2023, and the Security Target (Ref [6]). The certification report, certificate of the product being evaluated and the security target can be assessed on the MyCC Scheme Certified Product Register (MyCPR), which is available on the MyCC website at https://iscb.cybersecurity.my/index.php and these documents are also posted on Common Criteria Portal at http://www.commoncriteriaportal.org .

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 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	01 June 2023	All	Initial draft
v1	16 June 2023	All	Final Version
V1a	6 July 2023	All	Updated for V5.5

Executive Summary

The Target of Evaluation (TOE) is Trend Micro TippingPoint Threat Protection System (TPS) v5.5. The TOE is a network security platform that offers threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks (Intrusion Prevention System (IPS) capabilities). TPS provides coverage across various threat vectors, including advanced threats, malware, and phishing attempts. It employs a combination of technologies, such as deep packet inspection, threat reputation, and malware analysis, on a flow-by-flow basis, to detect and prevent attacks on the network.

The scope of the evaluation is defined by the Security Target (Ref[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. 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 SEF and the evaluation was completed on 26 May 2023.

Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed on MyCC Scheme Certified Products Register (MyCPR) and on Common Criteria Recognition Arrangement portal.

It is the responsibility of the user to ensure that Trend Micro TippingPoint Threat Protection System (TPS) v5.5 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and to this Certification Report prior deciding to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is the Trend Micro TippingPoint Threat Protection System (TPS) v5.5. It may also be referred to as TippingPoint Threat Protection System or simply TPS. TPS is a network security platform that offers threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks (Intrusion Prevention System (IPS) capabilities).

2 TPS provides coverage across various threat vectors, including advanced threats, malware, and phishing attempts. It employs a combination of technologies, such as deep packet inspection, threat reputation, and malware analysis, on a flow-by-flow basis, to detect and to prevent attacks on the network.

3 The product consists of the Threat Suppression Engine (TSE), Traffic Management filters, and Digital Vaccine (DV) filters that provide threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks.

4 The TOE's specialized hardware-based traffic classification engines enable the IPS to filter accurately at gigabit speeds and microsecond latencies. Unlike software-based systems whose performance may be affected by the number of filters installed, the scalable capacity of the TOE's hardware engine allows thousands of filters to run simultaneously with no impact on performance or accuracy. The TOE was evaluated as an IPS network device and does not include evaluation of the aforementioned speed or latency claims.

5 The TPS version 5.5 appliances included in the evaluation are TPS 1100TX, TPS 5500TX, TPS 8200TX, TPS 8400TX, and vTPS. Each physical appliance includes an RJ-45 console port and a 1 GbE copper management port. 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 concept of IO modules is not applicable to the vTPS model which has two virtual data ports.

6 The vTPS model 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. Each vTPS supports one vNIC (Vmware) or one bridge interface (KVM) for management.

7 All models (hardware and virtual) provide the same security protections and support all the functionality specified in this ST.

8 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 authorized 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.).

9 The TOE uses NIST validated cryptographic algorithms and must be configured to operate in FIPS mode in order to use them.

1.7 TOE Identification

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

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C128
TOE Name	Trend Micro TippingPoint Threat Protection System (TPS)
TOE Version	V5.5
Security Target Title	Trend Micro TippingPoint Threat Protection System (TPS) v5.5 Security Target
Security Target Version	V1.0
Security Target Date	22 May 2023
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])

Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, The United States of America
Developer	Trend Micro Incorporated 11305 Alterra Parkway, Austin, Texas 78758 USA
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

1.7 Security Policy

11 There are two (2) organisational security policies defined regarding the use of TOE.

Table 2: Security Organisational Policies

Policies	Statement
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

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

1.4.1 Logical Boundaries

13 The logical boundary of the TOE is summarized below:

- Security Audit

  The TOE is able to 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 space available for storage of audit records exceeds 75% space remaining threshold.

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

- Identification & Authentication

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

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

  The TOE provides authentication failure handling for remote administrator access. When the defined number of unsuccessful authentication attempts has been reached, the remote administrator accessing the TOE via SSH is locked out

for an administrator configurable period of time. Authentication failures by remote administrators cannot lead to a situation where no Administrator access is available to the TOE since administrator access is still available via local console.

- Security Management

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

  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.

- TOE Access

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

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

- 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.

- 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

14 The TOE is a self-contained hardware appliance or VM with TPS 5.5 software. The following table identifies the hardware appliance models included in the TOE.

Table 3: TOE Hardware Appliances

Device	Main Processor	Storage	Network Ports	Operating System / Software
TPS1100TX	Intel Pentium D-1517 (Broadwell with AES-NI) CPU / 4 Cores, 8 Threads, 1.6GHz, 25W TDP	Storage = 8GB CFAST (Internal) / 8GB (External)	One IOM Slot Hot-Swappable Up to 6 1GE Segments, Up to 4 10GE Segments, 1 40GE Segment	Linux-4.14.76-yocto-standard OpenSSL 1.0.2l-fips
TPS5500TX	Intel Xeon D-1559 (Broadwell with AES-NI) CPU / 12 Cores, 24 Threads, 1.5GHz, 45W TDP	Storage = 32GB CFAST (Internal) / 32GB (External)	Two IOM Slots, Hot-Swappable Up to 12 1GE Segments, Up to 8 10GE Segments, Up to 2 40GE Segments	Linux-4.14.76-yocto-standard OpenSSL 1.0.2l-fips
TPS8200TX	2x Intel Xeon E5-2648Lv3 (with AES-NI) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W TDP	Storage = 32GB CFAST (Internal) / 32GB (External)	Four IOM Slots, Two Hot-Swappable Up to 12 1GE Segments, Up to 8 10GE Segments, Up to 2 40GE Segments	Linux-4.14.76-yocto-standard OpenSSL 1.0.2l-fips
TPS 8400TX	2x Intel Xeon E5-2648Lv3 (with AES-NI) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W TDP	Storage = 32GB CFAST (Internal) / 32 GB (External)	Four IOM Slots, Hot-Swappable Up to 24 1GE Segments, Up to 16 10GE Segments, Up to 4 40GE Segments	Linux-4.14.76-yocto-standard OpenSSL 1.0.2l-fips

15 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.

16 Virtual Machine appliance TOEs consist of TPS v5.5, including Linux-4.14.76-yocto-standard and OpenSSL 1.0.2l-fips and requires the following:

Table 4: TOE Virtual Machine Appliances

Device	Image	Number of vCPUs	Memory	Disk	Operating System / Software
vTPS	Normal Option: • Vmware: vTPS_vmw_5.5.0_xxxx.zip Or • KVM: vTPS_kvm_5.5.0_xxxx.tar.gz	2– 3	8GB	16.2GB	ESXi Hypervisor version: Version 6.7 or 7.0.2 (only paid versions supported) or RHEL version 7.1 KVM
	Performance Option: • Vmware: vTPS_vmw_5.5.0_xxxx.zip Or • KVM: vTPS_kvm_5.5.0_xxxx.tar.gz	6	16GB	16.2GB	ESXi Hypervisor version: Version 6.7 or 7.0.2 (only paid versions supported) or RHEL version 7.1 KVM

vTPS virtual appliances are supported on hosts with Intel Haswell-based or Ivy Bridge-based microprocessors.

17 Software Requirements

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

· Vmware ESXi 6.7 or 7.0.2 (only paid versions supported)

· RHEL version 7.1 KVM

18 Additional Hardware Requirements

· External audit storage requires the use of syslog servers.

· An administrative workstation or terminal emulator equipped with SSH client software.

19 Exclusions

- 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 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.

1.5 Clarification of Scope

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

21 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]).

22 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

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

1.6.1 Operational Environmental assumptions

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

Table 5: Assumptions for the TOE Environment

Environment	Statement
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.
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. This protection is assumed to be sufficient to protect the device and the data it contains.
A.TRUSTED_ADMINISTRATOR	The authorized 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. 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 is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

1.7 Evaluated Configuration

25 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.

26 As stated in the ST (Ref. [6]) the TOE consists of a single standalone hardware or virtual appliance, each with v5.5.0. The hardware appliances are provided with the software and standard I/O modules pre-installed.

27 The TOE is a standalone hardware or virtual appliance and comprises one main subsystem providing the TOE Security Functions (TSFs). The TippingPoint Threat Protection System subsystem consists as following:

- TippingPoint appliance hardware or virtual machine – appliances include the TPS 5.5. software and a hardened Linux-4.14.76-yocto-standard operating system. All hardware models also include external user disk memory (CFast or SSD) while

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 concept of IO modules is not applicable to vTPS which has two virtual data ports. It also incorporates an OpenSSL cryptographic module to provide support respectively for Secure Shell (SSH) cryptographic protocols. The TPS subsystem provides all of the TSF including the Intrusion Prevention System (IPS) capabilities provided by the included Threat Suppression Engine (TSE), Traffic Management filters, and Digital Vaccine (DV).

28 Communication between the TPS and remote syslog server is secured using SSH.

29 The TOE provides a trusted path for administrators of the TOE to communicate with the TOE. The trusted path is implemented using SSH for access to the CLI. Administrators initiate the trusted path to the CLI by establishing an SSH connection using an SSH client (e.g., putty). The CLI can also be accessed via direct access to the TOE.

30 A sample deployment scenario is as follows.

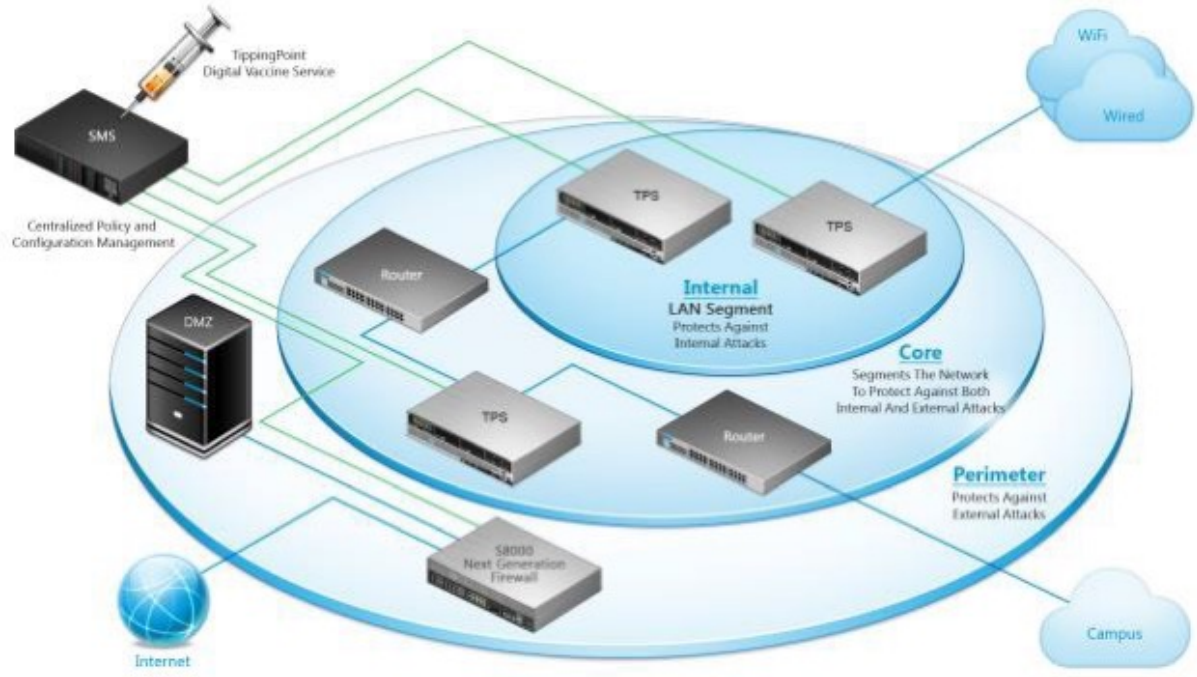

Figure 1 – Sample TPS Network Deployment Scenario

1.8 Delivery Procedures

31 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.

32 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

33 Delivery requirements call for system controls and procedures that provide assurance in the delivery of the TOE without any undetected tampering or interference. For a valid delivery, what is received by the end customer must correspond precisely to the TOE master copy, thus avoiding any tampering with the actual version, or substitution of a false version. Several procedures are necessary to maintain security when distributing versions of the TOE or parts of it to a user's site.

1.8.2 Delivery to Customers

34 Hardware

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.

35 Software Downloads and Updates

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 is used for the encryption.

- When the package is loaded onto the device, key exchanges occur and the package is unpacked, provided the keys match. If they don't, 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).

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

1.8.3 Method of Packaging and Shipment

36 Packaging

Trend Micro packages and labels the product in accordance with the current bill of material (BOM) and any applicable package specification for the product to be shipped.

All products are enclosed in cardboard shipping boxes and sealed with tape. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the shipping box.

Each hardware device is wrapped in a plastic bag and sealed with a warning label. The device cannot be removed from the plastic bag without damaging either the bag or the label.

37 Shipping

Trend Micro employs its current default carrier to deliver the product to customers. Trend Micro determines the best carrier, routing, and cost for the shipment.

Trend Micro's default carrier is currently UPS. Unless otherwise specified, all items are sent via UPS.

38 Tracking

Packages are tracked via the carrier's tracking numbers. The tracking number allows any party to find the status of the package either by calling the toll-free number or logging into the website. Tracking numbers are only provided to customers upon request.

2 Evaluation

39 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (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

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

2.1.1 Life-cycle support

41 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.

42 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

43 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

44 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

45 The evaluators examined the TOE security architecture description; they 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.

46 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

47 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

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

2.1.4 IT Product Testing

49 Testing at EAL 2 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 Plan Report.

2.1.4.1 Assessment of Developer Tests

50 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 evidences submitted.

2.1.4.2 Independent Functional Testing

51 At EAL 2, 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.

52 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 6: Independent Functional Test

Test ID	Description	Security Function	Results
F001 – Identification and Authentication	1. To test that the TOE requires each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user 2. To test the TSF's ability to detect when unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely using a password. 3. To test the TSF's ability to provide the password management capabilities meet FIA_PMG_EXT.1 requirements 4. To test the TSF's ability to provide only obscured feedback to the administrative user while the authentication is in progress at the local console. 5. To test the TSF's ability to provides local password-based and SSH public key-based authentication for administrative user authentication.	FIA_AFL.1 FIA_PMG_EXT.1 FIA_UAU.7 FIA_UAU_EXT.2 FIA_UIA_EXT.1	Passed.

Test ID	Description	Security Function	Results
F002 – Security Management	1. To test that the TOE capable of performing the management function meets FMT_SMF.1.1/Core requirements. 2. To test the TSF's ability to restrict the functions to Security Administrators to perform manual updates, modify behavior, and manage data.	FMT_MOF.1/ManualUpdate FMT_MOF.1/Functions FMT_MTD.1 & FMT_SMF.1/Core FMT_SMF.1/IPS FMT_SMR.2	Passed.
F003 – Security Audit	1. To test that the TOE able to generate record within each audit record and IPS records for the auditable 2. To test that the TOE able to provide reliable time 3. Stamps 4. To test that TSF be able to transmit audit data to external IT entities using a trusted channel. 5. To test that the TSF able to generate a warning to inform the Administrator before the audit trail exceeds storage capacity	FAU_GEN.1/Audit FAU_GEN.2 FAU_GEN.1/IPS FAU_STG.1 FAU_STG_EXT.1 FAU_STG_EXT.3 FTP_ITC.1	Passed.
F004 – Cryptographic Support and Trusted Path	1. To test the TSF able to implement SSH protocol that complies to FCS_SHC_EXT.1 and FCS_SHC_EXT.1 2. To test that TSF able to ensure that SSH transport implementation uses encryption algorithms defined in FCS_SHC_EXT.1 and FCS_SHC_EXT.1. 3. To test that the TSF shall ensure that the SSH transport implementation uses hmac-sha1, hmac-sha2-256, hmac-sha2-512 as its data integrity MAC algorithms and rejects all other MAC algorithms.	FCS_COP.1/DataEncryption FCS_COP.1/Hash FCS_COP.1/KeyedHash, FCS_RBG_EXT.1 FCS_SHC_EXT.1 FCS_SHS_EXT.1	Passed.

Test ID	Description	Security Function	Results
	4. To test that TSF 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 as described in RFC 4251 section 4.1. 5. To test that TSF able to provide a trusted communication channel that is distinct from other channels and provides assured identification of its end points and protection of channel data from modification or disclosure. 6. To test that the TOE permits remote users to initiate communication via the trusted path 7. To test that TSF shall initiate communication via the trusted channel for transmitting audit records to an external audit server.		Passed.
F005 – TSF Protection	1. To test that TSF able to store administrative passwords in non-plaintext form 2. To test that TSF able to prevent reading of all pre-shared keys, symmetric key, and private keys. 3. To test that TSF able to provide reliable time stamps for its own use. 4. To test TSF's ability to run self-tests to demonstrate correct operation.	FPT_APW_EXT.1 FPT_SKP_EXT.1 FPT_STM_EXT.1 FPT_TST_EXT.1 FPT_TUD_EXT.1	Passed.

Test ID	Description	Security Function	Results
	5. To test that TSF able to provide Security Administrators the ability · to query the currently executing version of the TOE firmware/software · ability to manually initiate updates to TOE firmware/software 6. To test that TSF able to provide a digital signature to authenticate firmware/software updates to the TOE.		
F006 – TOE Access	1. To test that TSF able to terminate local and remote interactive sessions after an inactivity time interval. 2. To test that TSF allow Administrator initiated termination of the Administrator's own interactive session 3. To test that TSF can display a Security Administrator-specified warning message before establishing an administrative user session.	FTA_SSL.3 FTA_SSL.4 FTA_TAB.1 FIA_UIA_EXT.1	Passed.
F007 – Intrusion Prevention System	1. To test that TSF able to support the definition of anomaly activity 2. To test that TSF able to allow the operations to be associated with anomaly-based IPS policies complies to IPS_ABD_EXT.1.3. 3. To test that TSF able to configure and implement known-good and known-bad IP addresses. 4. To test that TSF allows Security Administrators to configure IPS policy elements. 5. To test that TSF able to analyse IP-based network traffic and detect violations of IPS policies.	IPS_ABD_EXT.1 IPS_IPB_EXT.1 IPS_NTA_EXT.1 IPS_SBD_EXT.1	Passed.

Test ID	Description	Security Function	Results
	6. To test that TSF able to inspect network traffic protocols to satisfy IPS_NTA_EXT.1.2 7. To test that TSF able to assign signatures to promiscuous and inline sensor interfaces and designate one or more interfaces as 'management' for communication between TOE and external entities. 8. To test that TSF able to inspect packet header contents and header fields. 9. To test that TSF able inspect packet payload data to perform string-based pattern-matching. 10. To test that TSF able to detects header-based signatures at IPS sensor interfaces. 11. To test that TSF able to detect and apply traffic-pattern detection signatures to IPS sensor interfaces. 12. To test that TSF allows operations to be associated with signature-based IPS policies. 13. To test that TSF able to detect malicious payload even if it is split across multiple packets.		

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

2.1.4.3 Vulnerability Analysis

54 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.

55 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 equipment required for exploitation

2.1.4.4 Vulnerability testing

56 The penetration tests focused on:

a) Connectivity Check

b) Traceroute IP

c) Port Scanning

d) Banner Grabbing

e) Nessus Scanning

f) Packet Crafting

g) Vulnerability Dependency Check

h) UDP Flooding Attack

57 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 the Security Target (Ref [6]).

2.1.4.5 Testing Results

58 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 the test conducted were PASSED as expected.

3 Result of the Evaluation

59 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) v5.5 which is performed by Securelytics SEF.

60 Securelytics SEF found that Trend Micro TippingPoint Threat Protection System (TPS) v5.5 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.

61 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

62 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

63 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.

64 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Comments/Recommendations

65 The Malaysian Certification Body (MyCB) notes that:

a) Potential purchasers of the TOE should make themselves familiar with the developer guidance documentation provided with the TOE and pay attention to all security warnings.

b) Potential purchasers of the TOE 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) System Auditor should review the audit trail generated and exported by the TOE periodically.

d) Potential purchasers of the TOE should ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

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 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1a, CyberSecurity Malaysia, January 2023.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

[6] Trend Micro TippingPoint Threat Protection System (TPS) v5.5 Security Target, Version 1.0, 22 May 2023.

[7] Evaluation Technical Report, Version 1.0, 01 June 2023.

A.2 Terminology

A.2.1 Acronyms

Table 7: 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

Acronym	Expanded Term
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
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 8: 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 Guide 65

Term	Definition and Source
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.
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 ---