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

Version 1.0
July 14, 2023

Prepared for:

11305 Alterra Parkway
Austin, TX 78758

Prepared by:

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE references, TOE overview, and TOE description. It also contains the ST and TOE conformance claims, ST conventions, glossary, and list of abbreviations.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Trend Micro TPS offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the system security features. The following documents are available for download from the Trend Micro Online Help Center: https://docs.trendmicro.com/en-us/tippingpoint/threat-protection-system.aspx.
- Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, September 2020
- Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, November 2021
- Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, October 2021

The following document is available on the TOE's Product Compliant List web page on the NIAP web site:

- Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.5, 14 July 2023.
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
-

- TOE Summary Specification (Section 1)
-

- Protection Profile Claims (Section 1)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Trend Micro TippingPoint Threat Protection System (TPS) v5.5 Security Target

ST Version – 1.0

ST Date – July 14, 2023

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

The TOE consists of the following appliances running TPS software v5.5:

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

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

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

The vTPS virtual appliances consist of TPS v5.5, running on hosts with Intel Xeon CPUs based on Ivy Bridge or newer that support the RDRAND instruction and either

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

Evaluation testing of vTPS was conducted on the following platforms:

- ESXi 6.5 on Intel Xeon Silver 4116 (Skylake microarchitecture)
- KVM 1.5.3 on RHEL 7.5 on Intel Xeon Gold 6126 (Skylake microarchitecture).

The vTPS virtual appliances use virtual data ports and do not require I/O modules.

The vTPS appliances are provided as image files:

- vTPS_vmw_5.5.4_xxxx.zip (standard)
- vTPS_vmw_performance_v5.5.4_xxxx.zip (performance).

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- This TOE claims exact conformance to the collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020, [CPP_ND_V2.2E] including the following optional and selection-based SFRs:

FAU_STG.1, FAU_STG_EXT.3/LocSpace, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, and FMT_MOF.1/Functions.

The following NIAP Technical Decisions apply to this PP/ST and have been accounted for in the ST development and the conduct of the evaluation:

- TD0592 – NIT Technical Decision for Local Storage of Audit Records
- TD0591 – NIT Technical Decision for Virtual TOEs and hypervisors
- TD0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3
- TD0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e
- TD0572 – NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers
- TD0571 – NiT Technical Decision for Guidance on how to handle FIA_AFL.1
- TD0570 – NiT Technical Decision for Clarification about FIA_AFL.1
- TD0569 – NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7
- TD0564 – NiT Technical Decision for Vulnerability Analysis Search Criteria
- TD0563 – NiT Technical Decision for Clarification of audit date information
- TD0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN
- TD0538 – NIT Technical Decision for Outdated link to allowed-with list
- TD0536 – NIT Technical Decision for Update Verification Inconsistency

The following NIAP Technical Decisions do not apply to this ST/TOE:

- TD0556 – NIT Technical Decision for RFC 5077 question
  This TD is not applicable to the TOE. It affects FCS_TLSS_EXT.1, which is not claimed by the ST.
- TD0555 – NIT Technical Decision for RFC Reference incorrect in TLSS Test
  This TD is not applicable to the TOE. It affects FCS_TLSS_EXT.1, which is not claimed by the ST.
- TD0546 – NIT Technical Decision for DTLS - clarification of Application Note 63
  This TD is not applicable to the TOE. It affects FCS_DTLSC_EXT.1, which is not claimed by the ST.
- TD0537 – NIT Technical Decision for Incorrect Reference to FCS_TLSC_EXT.2.3
  This TD is not applicable to the TOE. It affects FCS_TLSC_EXT.2, which is not claimed by the ST.
- TD0528 – NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4
  This TD is not applicable to the TOE. It affects FCS_NTP_EXT.1, which is not claimed by the ST.
- TD0527 – Updates to Certificate Revocation Testing (FIA_X509_EXT.1)
  This TD is not applicable to the TOE. It affects the [NDcPP]'s iterations of FIA_X509_EXT.1, neither of which is claimed by the ST.

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
  - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).

  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Terminology

This section identifies TOE-specific terminology.

DV	Digital Vaccine
HA	High Availability
ISO	An ISO image (or .ISO file) is a computer file that is an exact copy of an existing file system
LSM	Local Security Manager
SMS	Security Management System
TPS	TippingPoint Threat Protection System (the TOE)

1.3.2 Abbreviations

This section identifies abbreviations and acronyms used in this ST.

AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher-Block Chaining
CA	Certificate Authority
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
NIST	National Institute of Standards and Technology
OS	Operating System
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
UAU	User Authentication
VM	Virtual Machine

2. TOE Description

The Target of Evaluation (TOE) is the TippingPoint Threat Protection System (TPS) v5.5. TPS is a network security platform that offers threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks. 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, in order to detect and prevent attacks on the network. 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. These threat protection functions may be enabled and used without affecting the claimed security functionality; however these features have not been evaluated. The TOE was evaluated as a network device only. The focus of this evaluation is on the TOE functionality supporting the claims in the collaborative Protection Profile for Network Devices [CPP_ND_V2.2E].

The security functionality specified in [CPP_ND_V2.2E] includes protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and use of NIST-validated cryptographic mechanisms.

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.

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.

All models (hardware and virtual) provide the same security protections and support all of the functionality specified in the [CPP_ND_V2.2E].

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

2.1 TOE Overview

The TippingPoint Threat Protection System v5.5 is a network device provided as a standalone hardware or virtual appliance. The appliances include the TPS 5.5.4 software.

Each appliance also includes the hardened Linux-4.14.76-yocto-standard operating system. All hardware models include external user disk memory (CFast or SSD) that is used to store all traffic logs, snapshots, ThreatDV URL Reputation Feed, User-defined URL Entries database, and packet capture data. The external memory can also be used for troubleshooting purposes. 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 and the 8200TX 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 IO modules is not applicable to vTPS which has two virtual data ports.

The TOE provides authorized administrators with a CLI accessible via SSH to manage the TOE and 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.

The authorized 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.

The TOE local and remote administration is provided through the Command Line Interface (CLI). The TOE supports Super User, Admin, and Operator roles that map to the Security Administrator role in the protection profile. Each user must be assigned a role in order to perform any management action.

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 Admin 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 Trend Micro support website and protected with a SHA-256 hash, and signed using 2048-bit RSA public/private key pair.

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.

A sample deployment scenario is as follows.

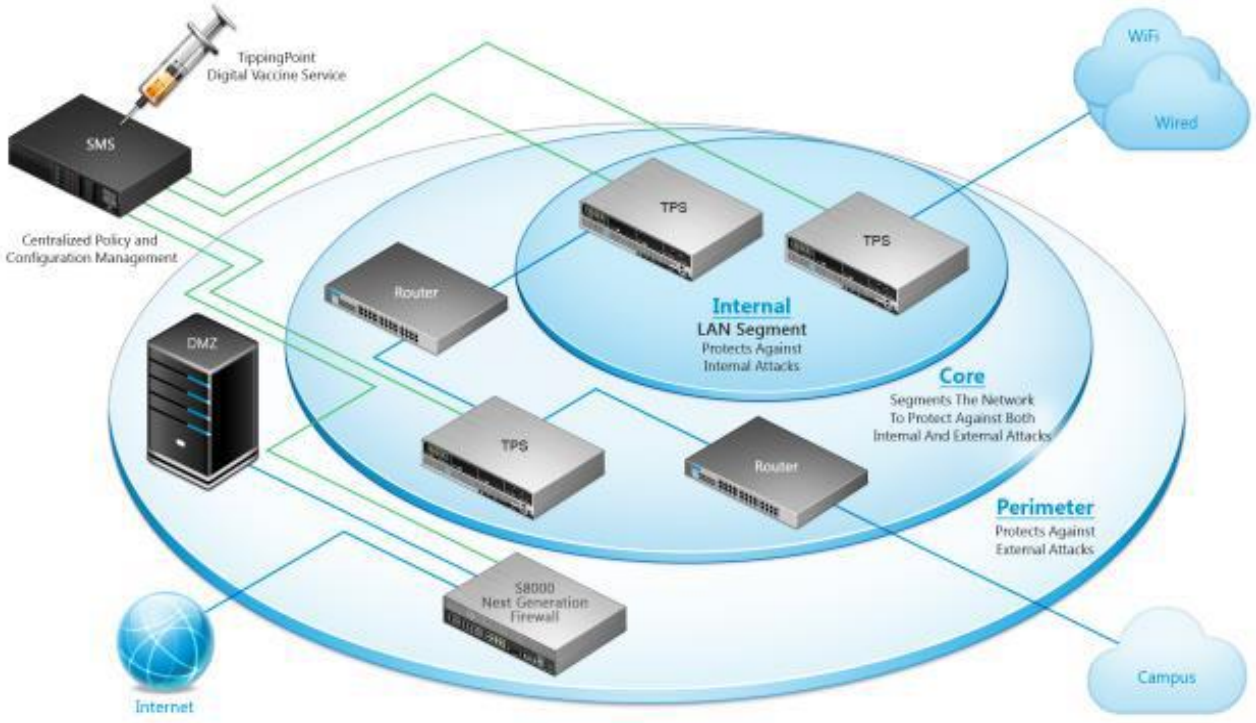

Figure 1 – Sample TPS Network Deployment Scenario

Figure 1 Sample TPS Network Deployment Scenario depicts an example of a corporate network with the TPS deployed to a variety of locations. A single TPS can be installed at the perimeter of the network, at the network core, on your intranet, or in all three locations. Though not depicted in the figure, the evaluated deployment includes a syslog server. The SMS appliance may be used in the evaluated configuration however it is not covered by the evaluation and no claims about its behavior are made. Note that the TOE is evaluated as a single appliance, not a distributed solution. A single appliance is sufficient for the TOE to address the claimed security functionality.

Deployment of multiple separate instances of the TOE is necessary only to ensure full coverage of network segments that require monitoring.

vTPS appliances are deployed to appropriate hardware that are located between L2 broadcast domains (VLANs or switches).

2.2 TOE Architecture

This section describes the TOE physical and logical boundaries.

2.2.1 Physical Boundaries

The TOE is a self-contained hardware appliance or VM with TPS 5.5.4 software.

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

Device	Main Processor	Storage	Network Ports	Operating System / Software
TPS1100TX	Intel Pentium D-1517 (Broadwell) 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) 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 (Haswell) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W 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
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 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

Table 1 TOE Hardware Appliances

The TippingPoint vTPS is deployed between layer 2 (L2) broadcast domains (virtual switches) using a Normal image or a Performance image. Performance image offers an increased capacity for vCPUs and threading.

Virtual Machine appliance TOEs consist of TPS v5.5.4, including Linux-4.14.76-yocto-standard and OpenSSL 1.0.2l-fips and requires the following:

Device	Image	Number of vCPUs	Memory	Disk	Operating System / Software
vTPS	Normal image: • VMware: vTPS_vmw_5.5.4_xxxx.zip	2 – 3	8GB	16.2GB	ESXi Hypervisor version: Version 5.5 (Patch 3116895), Version 6.0 (Patch 5572656), Version 6.5, Version 6.7, or RHEL version 7.1 KVM
	Performance image: • VMware: vTPS_vmw_performance_v5.5.4_xxxx.zip	6	16GB	16.2GB	ESXi Hypervisor version: Version 5.5 (Patch 3116895), Version 6.0 (Patch 5572656), Version 6.5, Version 6.7, or RHEL version 7.1 KVM

Table 2 TOE Virtual Machine Appliances

vTPS virtual appliances are supported on hosts with Intel Xeon CPUs based on Ivy Bridge or newer that support the RDRAND instruction.

2.2.1.1 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 5.5, or 6.0, or 6.5, or 6.7
- RHEL version 7.1 KVM

2.2.1.2 Additional Hardware Requirements

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

2.2.1.3 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 TPS intrusion prevention services including collection, inspection, analyzation, and reaction capabilities applied to network traffic have not been evaluated and no claims are made in relation to these functions. They may be used in the evaluated configuration without affecting the claimed security functions.

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.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

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

2.2.2.1 Security audit

The TOE is able to generate audit records for security relevant events specified in [CPP_ND_V2.2E]. 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.

2.2.2.2 Cryptographic support

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

2.2.2.3 Identification and authentication

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

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

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

2.2.2.4 Security management

The TOE provides administrator roles and supports local and remote administration. The TOE supports Super User, Admin, and Operator roles that map to the Security Administrator role in the claimed PP. Each user must be assigned a role in order to perform any management action. The TOE provides authorized administrators with a CLI accessible via SSH for TOE configuration and to monitor, collect, log, and react in real-time to potentially malicious network traffic.

2.2.2.5 Protection of the TSF

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

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

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

2.2.2.6 TOE access

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

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

2.2.2.7 Trusted path/channels

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

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

2.3 TOE Documentation

Trend Micro TPS offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the system security features. The following documents are available for download from the Trend Micro Online Help Center: https://docs.trendmicro.com/en-us/tippingpoint/threat-protection-system.aspx.

- Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, September 2020
- Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, November 2021
- Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, October 2021

The following document is available on the TOE's Product Compliant List web page on the NIAP web site:

- Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.5, 14 July 2023.

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the [CPP_ND_V2.2E], excluding A.COMPONENTS_RUNNING, which is for distributed TOEs only.

In general, the [CPP_ND_V2.2E] has presented a Security Problem Definition appropriate for network infrastructure devices, and as such is applicable to the Trend Micro TPS TOE.

4. Security Objectives

Like the Security Problem Definition, this security target includes by reference the Security Objectives from the [CPP_ND_V2.2E], excluding OE.COMPONENTS_RUNNING (for distributed TOEs only). The [CPP_ND_V2.2E] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [CPP_ND_V2.2E] has presented a Security Objectives statement appropriate for network infrastructure devices, and as such is applicable to the Trend Micro TPS TOE.

4.1 Security Objectives for the Operational Environment

OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration.

If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from [CPP_ND_V2.2E], including the following optional and selection-based SFRs: FAU_STG.1, FAU_STG_EXT.3/LocSpace, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, and FMT_MOF.1/Functions.

As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [CPP_ND_V2.2E] made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary. Text deleted from SFRs by a refinement in [CPP_ND_V2.2E] is not reproduced in ST.

The SARs are the set of SARs specified in [CPP_ND_V2.2E].

5.1 Extended Requirements

All extended requirements in this ST have been drawn from the [CPP_ND_V2.2E]. The [CPP_ND_V2.2E] defines the following extended SFRs and since they are not redefined in this ST, the [CPP_ND_V2.2E] should be consulted for more information regarding those CC extensions.

- FAU_STG_EXT.1: External Audit Event Storage
- FAU_STG_EXT.3/LocSpace: Action in Case of Possible Audit Data Loss
- FCS_RBG_EXT.1: Random Bit Generation
- FCS_SSHC_EXT.1: SSH Client Protocol
- FCS_SSHS_EXT.1: SSH Server Protocol
- FIA_PMG_EXT.1: Password Management
- FIA_UIA_EXT.1: User Identification and Authentication
- FIA_UAU_EXT.2: Password-based Authentication Mechanism
- FPT_APW_EXT.1: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Protection of TSF Data (for Reading of all Pre-shared, Symmetric and Private Keys)
- FPT_STM_EXT.1: Reliable Time Stamps
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the Trend Micro TPS TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_STG.1: Protected Audit Trail Storage
	FAU_STG_EXT.1: Protected Audit Event Storage
	FAU_STG_EXT.3/LocSpace: Action in Case of Possible Audit Data Loss
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation

Requirement Class	Requirement Component
	FCS_CKM.2: Cryptographic Key Establishment
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/ Decryption)
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash : Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	FCS_RBG_EXT.1: Random Bit Generation
	FCS_SSHC_EXT.1: SSH Client Protocol
	FCS_SSHS_EXT.1: SSH Server Protocol
FIA: Identification and authentication	FIA_AFL.1: Authentication Failure Management
	FIA_PMG_EXT.1: Password Management
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_UAU_EXT.2: Password-based Authentication Mechanism
	FIA_UAU.7: Protected Authentication Feedback
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behaviour
	FMT_MOF.1/Functions: Management of Security Functions Behaviour
	FMT_MTD.1/CoreData: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Administrator Passwords
	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM_EXT.1: Reliable Time Stamps
	FPT_TUD_EXT.1: Trusted Update
	FPT_TST_EXT.1: TSF Testing
FTA: TOE access	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1/Admin: Trusted Path

Table 3 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions comprising:
- Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***]*;*

d) Specifically defined auditable events listed in Table 4.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 4.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.3/LocSpace	Low storage space for audit events.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSHC_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of the TSF data.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions	None.

Table 4 Auditable Events

5.2.1.2 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 Protected Audit Trail Storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

5.2.1.4 Action in Case of Possible Audit Data Loss (FAU_STG_EXT.3/LocSpace)

FAU_STG_EXT.3.1/LocSpace The TSF shall generate a warning to inform the Administrator before the audit trail exceeds the local audit trail storage capacity.

5.2.1.5 Protected Audit Event Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [

- ***The TOE shall consist of a single standalone component that stores audit data locally.***]

FAU_STG_EXT.1.3 The TSF shall [***overwrite previous audit records according to the following rule: [the oldest historical audit file is deleted, the current audit file is renamed as a historical audit file, and a new current audit file is created]***] when the local storage space for audit data is full.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: **[**

- ***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;***
- ***ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;***
- ***FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].***

].

5.2.2.2 Cryptographic Key Establishment (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- ***Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";***
- ***FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526]*[1]*.***

].

5.2.2.3 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For plaintext keys in volatile storage, the destruction shall be executed by a* [*single overwrite consisting of [zeroes]*];**
- ***For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that* [*logically addresses the storage location of the key and performs a [single] overwrite consisting of [a new value of the key]*]**

]
that meets the following: No Standard.

[1] Modified by TD0580

5.2.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (FCS_COP.1/Data Encryption)

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm [**AES used in *[CBC, GCM]*]** mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: [**AES as specified in ISO 18033-3**, ***[CBC as specified in ISO 10116, GCM as specified in ISO 19772]***].

5.2.2.5 Cryptographic Operation (Signature Generation and Verification) FCS_COP.1/SigGen

FCS_COP.1.1/SigGen The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- ***RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits*]**,
- ***Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits, 384-bits, 521-bits]***]

that meet the following: [

- ***For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***
- ***For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4***

].

5.2.2.6 Cryptographic Operation (Hash Algorithm) (FCS_COP.1/Hash)

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm **[*SHA-1, SHA-256, SHA-384, SHA-512*]** and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004].

5.2.2.7 Cryptographic Operation (Keyed Hash Algorithm) (FCS_COP.1/KeyedHash)

FCS_COP.1.1/KeyedHash The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512, implicit***] and cryptographic key sizes [**160, 256, 512 bits**] and message digest sizes [***160, 256, 512***] bits that meet the following: [ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"].

5.2.2.8 Random Bit Generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[two] platform-based noise sources***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.2.2.9 SSH Client Protocol (FCS_SSHC_EXT.1)

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, [***5647, 5656, 6668***].

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [***no other method***].

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [**256K**] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 The TSF shall 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***].

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa***, ***ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521***] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6 The TSF shall 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).

FCS_SSHC_EXT.1.7 The TSF shall ensure that [***diffie-hellman-group14-sha1***, ***ecdh-sha2-nistp256***] and [***ecdh-sha2-nistp384, ecdh-sha2-nistp521***] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall 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.

FCS_SSHC_EXT.1.9 The TSF shall 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 section 4.1.

5.2.2.10 SSH Server Protocol (FCS_SSHS_EXT.1)

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [***5647, 5656, 6668, 8268***].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [***password-based***].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [**256K**] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall 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***].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521***] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1***, ***hmac-sha2-256***, ***hmac-sha2-512***, ***AEAD_AES_128_GCM, AEAD_AES_256_GCM***] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [***diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512***] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall 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.

5.2.3 Identification and authentication (FIA)

5.2.3.1 Authentication Failure Management (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [**1 to 10**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed***].

5.2.3.2 Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ***[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“,”, “.”, “/”, “<”, “>”, “?”]];***

b) Minimum password length shall be configurable to between [**1]** and [**15]** characters**.**

Application Note: *The minimum password length can be configured to “1”, “8”, or “15” only.*

5.2.3.3 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.2.3.4 Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1 The TSF shall provide a local [***password-based, SSH public key-based***] authentication mechanism to perform local administrative user authentication.

5.2.3.5 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- **[*[send Echo Reply in response to Echo Request ICMP messages received at the Management interface]***].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative/ user.

5.2.4 Security management (FMT)

5.2.4.1 Management of Functions in TSF (FMT_MOF.1/ManualUpdate)

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

5.2.4.2 Management of Security Functions Behaviour (FMT_MOF.1/Functions)

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [***determine the behaviour of; modify the behaviour of***] the functions [***transmission of audit data to an external IT entity***] to Security Administrators.

5.2.4.3 Management of TSF Data (FMT_MTD.1/CoreData)

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.2.4.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;

[

- ***Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);***
- ***Ability to configure the cryptographic functionality;***
- ***Ability to set the time which is used for time-stamps;***

].

5.2.4.5 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

- Security Administrator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.2.5.2 Protection of TSF Data (for Reading of all Pre-shared, Symmetric and Private Keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.5.3 Reliable Time Stamps (FPT_STM_EXT.1)

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [***allow the Security Administrator to set the time***].

5.2.5.4 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)***] to demonstrate the correct operation of the TSF: [

- **software module integrity tests**

- **cryptographic known answer tests**

].

5.2.5.5 Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

FPT_TUD_EXT.1.2 The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.2.6 TOE access (FTA)

5.2.6.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.2.6.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.2.6.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.2.6.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.2.7 Trusted path/channels (FTP)

5.2.7.1 Inter-TSF Trusted Channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall be capable of using [***SSH***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***no other capabilities***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server**].

5.2.7.2 Trusted Path (FTP_TRP.1/Admin)

FTP_TRP.1.1/Admin The TSF shall be capable of using [***SSH***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

FTP_TRP.1.2/Admin The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administrative actions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the [CPP_ND_V2.2E].

Requirement Class	Requirement Component
ASE: Security Target	ASE_CCL.1: Conformance claims
	ASE_ECD.1: Extended components definition
	ASE_INT.1: ST introduction
	ASE_OBJ.1: Security objectives for the operational environment
	ASE_REQ.1: Stated security requirements
	ASE_SPD.1: Security Problem Definition
	ASE_TSS.1: TOE summary specification
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 5 Security Assurance Components

Consequently, the assurance activities specified in [CPP_ND_V2.2E] apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

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

6.1 Security Audit

The TOE is a single standalone component that generates security relevant audit records including administrative activity. The audit records are stored locally on the TOE, protected from unauthorized modification and deletion and can be sent to a remote syslog server for storage. The connection for transmission of audit records uses SSH.

6.1.1 FAU_GEN.1: Audit Data Generation

The TOE is able to generate audit records for security relevant events as they occur. The events that can cause an audit record to be logged include: starting and stopping the audit function; all attempts to initiate a secure communication channel; and any use of an administrator action via the CLI comprising:

- Administrative login and logout (including the name of the user account).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself, when a key is changed, it is uniquely identified in the audit log by being referenced as an SSH key and by identifying the username that the key is associated with).
- Resetting passwords (name of related user account is logged).
- Attempts to initiate a TOE update.
- Modification of the behaviour of the transmission of audit data to an external IT entity.

Additionally, the TOE generates an audit record warning that is written to the audit trail when the space allocated for storage of audit records exceeds 75% of capacity. This is default behavior and is not configurable.

The audit records include the following fields:

- Log ID - Displays the system-assigned log ID number.
- Log Entry Time - Displays the time the log was entered in the format YYYY-MM-DD HH:MM:SS.
- Device Name - The device name on which the session was logged.
- User - Displays the login name of the user who performed the audited action. The user listed for an event can include SYS and CLI.
- Access - Displays the access level of the user performing the action. This field is only present in Audit Log type.
- IP Address - Displays the IP address from which the user performed the action.
- Interface - Displays the interface with which the user logged in: CLI for the command line interface. For system-initiated actions, SYS displays in this field.
- Access - Displays the access level of the user performing the action (from 0 (no administrative permissions to 8 (super user)). In particular, the following values relevant to the TOE's evaluated configuration are defined for this field as follows:
    - 0 NORMAL_ACCESS (no administrative permissions)
    - 1 OPERATOR_ACCESS
    - 4 ADMINISTRATOR_ACCESS
    - 8 SUPER_USER_ACCESS

- Result - Displays the action performed or the result of a LOGIN or LOGOUT attempt.
- Action/Message – Text of the log entry identifying the action performed as a result. For example, Log Files Reset.

Table 4 corresponds to the audit events specified in Table 2 of the [CPP_ND_V2.2E] and includes the audit events specified in the [CPP_ND_V2.2E] for optional and selected SFRs as selected in this ST.

6.1.2 FAU_GEN.2: User Identity Association

For audit events resulting from actions of identified users, the TOE associates each auditable event with the identity of the user that caused the event. Specifically, user identity is captured by the 'User' and 'IP Address' fields in the audit records.

6.1.3 FAU_STG.1: Protected Audit Trail Storage

The TOE includes an internal log implementation that can be used to store audit records locally on the TOE. The local audit logs are stored on the TOE hard drive in either the 'Audit' log or the 'System' log. The System log records information about the software processes that control the device, including startup and shutdown of the TOE events. All other required audit events as identified in **Table 4** are stored in the Audit log.

Each TPS system including vTPS systems allocate approximately one eighth of the system's internal disk space for the audit log file. Systems that support less than 5Gbps inspection throughput have 8GB internal disk space while systems that support 5Gbps and above inspection throughput have 32GB internal disk space. This implies approximately 1GB audit log file disk space on TPS systems with less than 5Gbps and approximately 4GB on TPS systems greater than 5Gbps.

The enforced limits on the size of the audit data logs are specified as a percentage of internal log disk space using the **`log-file-size`** CLI setting. The maximum amount of audit data that are stored locally in each log cannot exceed this percentage and the combined percentage configured for the logs must equal 100%.

The audit records on the TOE are protected by database access control. There are no interfaces to modify or delete individual audit records. Only Super Users can configure the log sizes and clear the log files. The command: **`clear log-file`** deletes the locally stored Audit log. There are no interfaces to modify stored audit data.

6.1.4 FAU_STG_EXT.1: Protected Audit Event Storage

The TOE is capable of locally storing audit records and can be configured to send audit records to an external syslog server using SSH. When configured to send audit records to a syslog server, audit records are also written to the external syslog as they are written locally to the TOE audit log (in real-time).

Each TPS system including vTPS systems allocate approximately one eighth of the system's internal disk space for the audit log file. Systems that support less than 5Gbps inspection throughput have 8GB internal disk space while systems that support 5Gbps and above inspection throughput have 32GB internal disk space. This implies approximately 1GB audit log file disk space on TPS systems with less than 5Gbps and approximately 4GB on TPS systems greater than 5Gbps.

System disk space is monitored and once the available storage for audit trail exceeds 75% full an alert is generated. When audit storage space is exhausted, the TOE overwrites previous audit records by deleting the oldest historical log file, renaming the current log file to be a historical file, and creating a new current log file. There are 5 files by default for log rollover functionality (ex: audit.log -- current, audit.log.1..audit.log.4 -- rotated ones). Each file is allocated 20% of the total space allocated for that log. For example when the audit.log reaches its capacity (20% of audit log space) it is renamed to audit.log.1 and the new audit entries are written to audit.log. When audit.log reaches its capacity again, audit.log.1-->audit.log.2, audit.log-->audit.log.1 and new entries are written to audit.log. If all five files become filled (100% audit log space used) then the oldest file gets deleted.

6.1.5 FAU_STG_EXT.3/LocSpace: Action in Case of Possible Audit Data Loss

When the available storage for audit trail exceeds 75% full, the TOE generates an alert and writes it to the system log. This is default behavior and is not configurable.

6.2 Cryptographic Support

The TOE includes OpenSSL1.0.2l-fips wrapped with TippingPoint Crypto Core OpenSSL 2.0.13 library which provides cryptographic algorithms and services. The following functions have been certified in accordance with the identified standards. Note that two sets of algorithm certificates were awarded because the 1100TX and 5500TX were tested separately after their release.

Functions	Standards	Certificates
FCS_CKM.1 Cryptographic Key Generation		
• RSA (2048 bits)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	RSA # A2221
• ECDSA (P-256, P-384, P-521 curves)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	ECDSA # A2221
• FFC Schemes using 'safe-prime' groups (2048-bits, 3072-bits, 4096-bits)	NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and RFC 3526	N/A
FCS_CKM.2 Cryptographic Key Establishment		
• ECDSA (P-256, P-384, P-521 curves)	NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";	KAS # A2221
• FFC Schemes using 'safe-prime' groups (2048-bits, 3072-bits, 4096-bits)	NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and RFC 3526	N/A
FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)		
• AES CBC (128 and 256 bits)	ISO 18033-3, CBC as specified in ISO 10116	AES #A2221
• AES GCM (128 and 256 bits)	ISO 18033-3, GCM as specified in ISO 19772	AES # A2221
FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-4 "Digital Signature Standard (DSS)"	RSA #A2221
• ECDSA NIST curves (P-256, P-384, P-521)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves"; ISO/IEC 14888-3, Section 6.4	ECDSA #A2221
FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)		
• SHA-1 (digest size 160 bits) • SHA-256 (digest size 256 bits) • SHA-384 (digest size 384 bits) • SHA-512 (digest size 512 bits)	ISO/IEC 10118-3:2004	# A2221
FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)		

Functions	Standards	Certificates
• HMAC-SHA-1 (key size 160 bits and digest size 160 bits) • HMAC-SHA-256 (key size 256 bits and digest size 256 bits) • HMAC-SHA-512 (key size 512 bits and digest size 512 bits)	ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"	HMAC # A2221
FCS_RBG_EXT.1: Random Bit Generation		
• CTR-DRBG(AES) with two independent platform-based noise source of 256 bits of non-determinism	ISO/IEC 18031:2011	DRBG # A2221

Table 6 Cryptographic Functions

6.2.1 FCS_CKM.1: Cryptographic Key Generation

The TOE generates RSA asymmetric keys using cryptographic key sizes of 2048 bits according to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3. The RSA asymmetric keys are used in support of SSH public key authentication. See table above for Asymmetric key generation: RSA (2048-bit). The TOE generates asymmetric keys using FFC schemes using "safe-prime" groups in support of SSH key establishment. Diffie-Hellman groups 14, 15, and 16 are the supported key exchange methods and the key sizes are 2048 bits (Group 14), 3072 bits (Group 15), and 4096 bits (Group 16). The TOE also generates ECC asymmetric keys using NIST curves: P-256, P-384, P-521 in support of SSH public key authentication and SSH session establishment. Both key generation methods are used in communications with external syslog servers and with users accessing the SSH management interface.

6.2.2 FCS_CKM.2: Cryptographic Key Establishment

The TOE performs key establishment using Diffie-Hellman group 14 that implements 2048-bit MODP Group according to RFC 3526, Section 3; Diffie-Hellman group 15 that implements 3072-bit MODP Group according to RFC 3526, Section 3; Diffie-Hellman group 16 that implements 4096-bit MODP Group according to RFC 3526, Section 3; and Elliptic Curve Diffie-Hellman key agreement using the P-256, P-384, or P-521 curve when an SSH ciphersuite is negotiated. These key establishment methods are used during SSH session establishment with external audit server and with users accessing the SSH management interface.

See **Table 6 Cryptographic Functions** above for detail.

6.2.3 FCS_CKM.4: Cryptographic Key Destruction

The TOE uses the following secret keys, private keys and CSPs.

Key/CSP Name	Algorithm/Key Size	Description
RSA SGK	RSA 2048 bits	RSA signature generation key
RSA KDK	RSA 2048 bits	RSA key decryption key
ECC Keys	ECC key pair (P-256, P-384, P-521)	SSH session keys
SSH-RSA	RSA 2048 bits	SSH-RSA client keys
AES EDK	AES 128, 256 bits	AES encrypt/decrypt key
HMAC Key	HMAC-SHA-1 (160 bits) HMAC-SHA-256 (256 bits) HMAC-SHA-512 (512 bits)	HMAC keyed hash key
CTR_DRBG Key	AES 256 bits	Internal CTR_DRBG key variable

Table 7 Secret keys, Private keys and CSPs

The TOE incorporates OpenSSL, which provides implementation of the cryptographic algorithms specified in **Table 6**. The TOE operates in FIPS mode and invokes the OpenSSL crypto module APIs to set up and maintain the full SSH session, using the underlying cryptographic algorithms as identified in **Table 6**. Therefore, all key generation, negotiation of session keys, and packet authentication is performed and managed by the crypto module.

User passwords and SSH-RSA client keys are stored in internal flash, encrypted using AES with a 256 bit key encrypting key (KEK). When deleted, SSH_RSA client keys are overwritten with zeros. The KEK is stored on Compact Flash (CF) and is itself encrypted using AES with a 256 bit Master Key. For TPS appliances, the Master Key exists in hardware circuitry within the TOE. It is generated during manufacturing and is unique to each appliance.

For the vTPS, the Master Key is generated during software installation and stored on a system memory file. The vTPS implements multi-layer software obfuscation techniques (including masking and key wrapping) to protect the Master Key. These techniques protect the Master Key and associated authorization factors from unauthorized access. Anyone who has the copy of software or access to a running copy of software will not be able to access the plaintext Master Key by visually inspecting the software image, reverse engineering the software, or inspecting a memory footprint of a running software image. The Master Key and associated authorization factors are destroyed when the vTPS is factory reset (by execution of the debug factory-reset CLI command, or by deleting and reinstalling the VM). When this occurs, a new Master Key and authorization factors are generated, overwriting the previous values.

All remaining keys (see **Table 7** above) are plaintext stored in RAM, only during the lifetime of an API call. They are destroyed immediately after use, by overwriting the memory once with zeroes.

6.2.4 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

The TOE performs 128/256-bit AES encryption/decryption as specified in ISO 18033-3, CBC mode as specified in ISO 10116 and GCM mode as specified in ISO 19772.

6.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

The TOE will provide cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 bits that meets the FIPS 186-4 Digital Signature Standard. The TOE's SSH implementation supports the following public key algorithms for public key-based authentication: ecdsa-sha2-nistp256; ecdsa-sha2-nistp384; and ecdsa-sha2-nistp521 meeting the FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and ISO/IEC 14888-3, Section 6.4 standard.

6.2.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

The TOE performs SHA-1, SHA-256, SHA-384, SHA-512 cryptographic hashing services in accordance with ISO/IEC 10118-3:2004. The SHA hash algorithm is used as part of HMAC, but is also used as part of RSA digital signature creation and verification. SHA-256, SHA-384, and SHA-512 also support ECDSA signature generation and verification.

6.2.7 FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)

The TOE performs keyed-hash message authentication that meets the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2. The key length, hash function used, block size, and output MAC lengths are identified in the table below.

Algorithm	Key Size	Block Size	Message Digest Size
SHA-1	160	512	160
SHA-256	256	512	256
SHA-512	512	1024	512

Table 8 HMAC Properties

Keyed-hash message authentication services HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 are supported for SSH. SSH also uses implicit message authentication when the encryption algorithm is AES-GCM.

6.2.8 FCS_RBG_EXT.1: Random Bit Generation

The TOE uses a software-based deterministic random bit generator that complies with ISO/IEC 18031:2011, using CTR_DRBG (AES). The TOE seeds the DRBG with 256 bits of entropy. All platforms use entropy provided by the Linux kernel, including device, input, interrupt, disk randomness, and the RDRAND instruction.

6.2.9 FCS_SSHC_EXT.1 – SSH Client Protocol / FCS_SSHS_EXT.1 – SSH Server Protocol

The TOE acts as an SSH client for secure communications with an external audit server. The TOE acts as an SSH Server for secure communications with remote administrators. The TOE implements the SSHv2 protocol and complies with RFCs 4251, 4252, 4253, 4254, 5647, 5656, and 6668. The TOE's server implementation also implements RFC 8268.

Both of the TOE's client and server implementations of SSH support the public-key-based authentication method as described in RFC 4252. The TOE's SSH server implementation also supports password-based authentication as described in RFC 4252. The TOE drops packets greater than 256K bytes in an SSH transport connection as described in RFC 4253.

As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (256K bytes) the packet will be dropped.

The TOE's SSH transport implementation uses:

- aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com encryption algorithms
- ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,and ecdsa-sha2-nistp521 as its public key algorithms; and
- hmac-sha1, hmac-sha2-256, hmac-sha2-512 (implicit for aes*-gcm@openssh.com) as its MAC algorithms.

The SSH algorithms are enabled by default. The TOE rejects any encryption, public key and MAC algorithms not listed above. SSH ciphers can be toggled using the command: **debug ssh ciphers CIPHER enable/disable**. PK and MAC algorithms can be changed by modifying the sshd config file as root.

The TOE's SSH client uses diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 as its key exchange methods. The TOE's SSH server uses diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, and diffie-hellman-group16-sha512 as its key exchange methods. The TOE ensures that the SSH connection is rekeyed when a threshold of either one hour has been reached, or when one gigabyte of data has been transmitted. Both thresholds are checked by the TOE and rekeying is performed upon reaching the threshold that is hit first.

The TOE requires users to be identified and authenticated before they can access any of the TOE functions.

6.3 Identification and Authentication

The TOE provides identification and authentication and password management functions.

6.3.1 FIA_AFL.1 Authentication Failure Management

The TOE can detect when an Administrator (Super User and Admin) configurable number (from 1 to 10) of failed remote authentication attempts has been reached. 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 (Super User and Admin) configurable period of time (1-1440 minutes). Authentication failures by remote Administrators cannot lead to a situation where no Administrator access is available to the TOE. If remote administrators are locked out, administrator access is still available via local console. This prevents any condition where no administrator access is available.

6.3.2 FIA_PMG_EXT.1: Password Management

The TOE can be composed of passwords from any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “,”, “.”, “/”, “<”, “>”, “?”. Single and double quotes, spaces or back slashes are not allowed. The minimum password length is administrator configurable to 1, 8 or 15 characters, depending on Password Security Level.

The TOE offers configurable global authentication settings that apply to all users. The TOE offers pre-defined Password Security Levels of None, Low, Medium and High. The default value is Medium. Each level adopts the requirements of the preceding level and adds additional requirements for the user name and password.

A Password Security Level of None does not contain any restrictions other than User names cannot contain spaces. The Password Security Level of Low requires User names to be at least six characters in length; a new password must be different than the current password, and passwords must be at least eight characters in length. A Password Security Level of Medium specifies the following additional password complexity requirements:

- Contains at least two alphabetic characters,
- Contains at least one numeric character, and
- Contains at least one non-alphanumeric character.

A Password Security Level of High requires the passwords to be at least 15 characters and meet the following additional password complexity requirements:

- Contains at least one uppercase character,
- Contains at least one lowercase character, and
- At least half the characters cannot occupy the same positions as the current password.

Based on the configured password security level, the only security-relevant condition is the enforced length configured by level.

6.3.3 FIA_UAU.7: Protected Authentication Feedback

When logging in, the TOE does not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

6.3.4 FIA_UIA_EXT.1: User Identification and Authentication, FIA_UAU_EXT.2: Password-based Authentication Mechanism

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 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.

In order to log in, the user must provide an identity and also 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. Users are authenticated directly by the TOE. Any resulting session is dependent upon successful authentication and established sessions are associated with the role(s) (see Section 6.4) assigned to the user.

6.4 Security Management

The TOE provides a CLI to access the security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE. The TOE controls user access to the TOE and resources based on user role. Users are given permission to access a set of commands and resources based on their user role.

6.4.1 FMT_MOF.1/ManualUpdate: Management of Security Functions Behaviour Requests

The initiation of manual TOE updates is restricted to the Admin and Super User roles.

6.4.2 FMT_MOF.1/Functions: Management of Security Functions Behaviour

Users with the Super User, or Admin roles can configure the audit data to be transmitted to a remote syslog server.

6.4.3 FMT_MTD.1/CoreData: Management of TSF Data

The ability to manage the TSF data is restricted to the Administrators. No administrative functions are accessible prior to administrator log-in. The authorized administrator must have the appropriate permissions as defined by the role to access the TSF data.

6.4.4 FMT_SMF.1: Specification of Management Functions

All administrative functionality is available from the CLI (locally or remote).

The TOE provides the following management functions:

- Configure the access banner;
- Configure the cryptographic functionality (cryptographic ciphers used in SSH sessions);
- Set the time which is used for time-stamps;
- Update the TOE, and to verify the updates using the digital signature capability prior to installing those updates;
- Configure the authentication failure parameters for FIA_AFL.1;
- Configure the session inactivity time before session termination; and
- Configure audit behaviour (send audit records to a remote syslog server).

6.4.5 FMT_SMR.2: Restrictions on Security Roles

The TOE includes pre-defined administrator roles and supports local and remote administration. The pre-defined roles Super User, Admin, and Operator map to the Security Administrator role in the [CPP_ND_V2.2E]. The Operator role only has the ability to view TSF data as specified by FMT_MTD.1/CoreData. The Super User, and Admin have full access to manage the TOE as specified in FMT_SMF.1.

The TPS appliance has a serial console interface as well as an Ethernet interface dedicated to management. An administrator can manage the TOE locally via the CLI through the console interface. In addition, the CLI can be accessed remotely via SSH.

6.5 Protection of the TSF

The TOE ensures that sensitive information such as passwords and cryptographic keys are stored such that they are not accessible even to an administrator. The TOE provides its own internal clock which it uses to provide a reliable time source for audit records.

The TOE includes functions to perform self-tests and mechanisms for the update of the TOE software/firmware and verification of the cryptographic functions.

6.5.1 FPT_APW_EXT.1: Protection of Administrator Passwords

The TOE stores administrative passwords using 256-bit AES and prevents reading of plaintext passwords. The TOE does not offer any functions that will disclose to any users a plaintext password. See Section 6.2 for more information about stored passwords.

6.5.2 FPT_SKP_EXT.1: Protection of TSF Data (for Reading of all Pre-shared, Symmetric and Private Keys)

The TOE does not offer any functions that will disclose to any users a stored cryptographic key. See Section 6.2 for more information about stored keys.

6.5.3 FPT_STM_EXT.1: Reliable Time Stamps

The TOE is a hardware appliance or a virtual appliance image installed on a hardware appliance that includes a hardware-based real-time clock to ensure that reliable time information is available. The TOE's real-time clock is a Complementary Metal-Oxide Semiconductor that stores the system time and date information. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The clock is used for audit record time stamps, measuring session activity for termination, and for cryptographic operations based on time/date.

6.5.4 FPT_TST_EXT.1: TSF Testing

The TOE performs all self-tests (software module integrity tests and cryptographic known answer tests) on start-up. The TOE process manager service is responsible for bringing up all relevant TOE processes. All binaries include an embedded integrity checksum (md5sum) that the process manager verifies before starting the process. If a module fails a software integrity test, the TOE reports status indicating which failure occurred and transitions to an error state, in which the module ceases to continue processing.

The TOE includes the OpenSSL 2.0.13 FIPS wrapper which forces the execution of the self-tests and ensures the correct operation of cryptographic functions. OpenSSL performs the following cryptographic self-tests during start-up:

- Cryptographic known answer tests: for symmetric and one-way cryptographic operations, the TSF will process known input data and compare it to the pre-computed output for each algorithm to ensure results are consistent with known answers.
- Pairwise consistency tests: for public key cryptographic operations, the TSF will perform a cryptographic operation followed by its reverse (e.g. encrypt/decrypt; sign/verify) to ensure that the result of the calculation is the same as the initially-supplied value.

6.5.5 FPT_TUD_EXT.1: Trusted Update

The administrator uses the CLI to update the TOE, and to query the currently executing software version of the TOE. The command **version** displays the current software version.

The administrator uses a Debug command (**debug upgrade**) to download a TOE update package directly from a specified URL. The update package is published on Trend Micro support website. The vendor generates a digital signature of the update package by first calculating the SHA-256 hash of the update package, then encrypting the generated hash using its 2048-bit RSA private key. The TOE update package includes the digital signature and the public key is included in the software image. The digital signature is verified by the TOE prior to the package being installed. The process is as follows: the TOE calculates its own SHA-256 hash of the update package, then decrypts the digital signature accompanying the update package using the RSA public key matching the vendor's private key, and comparing the hash it calculated with the decrypted hash value. If they are equal, the package is valid and has not been modified. The digital signature is downloaded as part of the update package, and the TOE is pre-installed with the public key. The TOE starts the update process once it verifies the signature/hash. A package with an invalid signature will not be installed by the TOE.

6.6 TOE Access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session. The TOE can also enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated. Finally, the TOE allows administrators to terminate their own session.

6.6.1 FTA_SSL.3: TSF-initiated Termination

The TOE can be configured by an administrator to set an interactive remote session timeout value (any integer value greater than zero in minutes) for user sessions. The default timeout is 15 minutes. Note also that should a user have their session terminated (e.g., due to inactivity), they are required to successfully authenticate, by reentering their identity and authentication data, in order to establish a new session.

The TOE can be configured by an administrator to set an interactive session timeout value for remote user sessions. The timeout value is in minutes and can be set to any integer value from 1 to 32000.

6.6.2 FTA_SSL.4: User-initiated Termination

Administrators can terminate their own interactive sessions by logging out at the console and SSH.

6.6.3 FTA_SSL_EXT.1: TSF-initiated Session Locking

The TOE can be configured by an administrator to set an interactive session timeout value for local user sessions. The timeout value is in minutes and can be set to any integer value from 1 to 32000.

The TOE implements the session inactivity limit for local interactive sessions at the console. Such sessions will be terminated when the inactivity period expires. Should a user have their session terminated (e.g., due to inactivity), they are required to successfully authenticate, by reentering their identity and authentication data, in order to establish a new session.

6.6.4 FTA_TAB.1: Default TOE Access Banners

The TOE supports an administrator-configurable TOE access banner that is displayed prior to a user completing the login process at the CLI. The banner text is configured using the **`login-banner`** command and the same text is displayed at both local and remote management connections (console, SSH).

6.7 Trusted Path/Channels

An authorized administrator can establish a secure remote connection with the TOE using SSH.

The TOE also uses SSH secure communications with an external log server to prevent unintended disclosure or modification of audit records.

6.7.1 FTP_ITC.1: Inter-TSF Trusted Channel

The TOE can be configured to export audit records to an external audit server. The TOE uses SSH to protect communications between itself and the audit server. SSH provides assured identification of its end points via host name/public key association as per FCS_SSHC_EXT.1.9 and protection of the channel data from disclosure and detection of modification of the channel data. The TOE initiates communication via the trusted channel for the audit server.

The TOEs secure protocols are supported by FIPS Approved cryptographic mechanisms included in the TOE implementation.

6.7.2 FTP_TRP.1/Admin: Trusted Path

The TOE protects interactive communication with administrators accessing the CLI using SSH, which provides confidentiality of transmitted information and detects any loss of integrity. Remote administrators initiate communication via the trusted path by using an SSH client to login.

To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to access the CLI features. Remote administrators may alternatively need to provide an SSH key for key-based authentication. The trusted path is used for initial Administrator authentication and all subsequent administrative actions.

The secure protocols are supported by FIPS-approved cryptographic mechanisms included in the TOE implementation.

7. Protection Profile Claims

The ST claims exact conformance to the collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020, [CPP_ND_V2.2E] including the following optional and selection-based SFRs: FAU_STG.1, FAU_STG_EXT.3/LocSpace, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, and FMT_MOF.1/Functions.

As explained in Sections 3 and 4, the Security Problem Definition and the Security Objectives of the [CPP_ND_V2.2E] have been included by reference into this ST.

All Security Functional Requirements (SFRs) in this ST have been reproduced from the [CPP_ND_V2.2E] and operations completed as appropriate.

8. Rationale

This ST includes by reference the [CPP_ND_V2.2E] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The ST makes no additions to the [CPP_ND_V2.2E] assumptions. [CPP_ND_V2.2E] security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [CPP_ND_V2.2E] application notes and evaluation activities. The security target did not add or remove any mandatory security requirements. Consequently, [CPP_ND_V2.2E] rationale applies and is complete.