Common Criteria Evaluated Configuration Guide (CCECG) for Threat Protection System (TPS) v5.5.0

Trend Micro™ TippingPoint™ Threat Protection System

Document Version 1.0

22 May 2023

Table of Contents

1 Introduction

This document provides administrative guidance information for the Trend Micro™ TippingPoint™ Threat Protection System. This document describes preparative and operational procedures for the use of the Trend Micro TippingPoint Threat Protection System in its Common Criteria evaluated configuration. This document is a supplement to the Trend Micro TippingPoint Threat Protection Command Line Interface Reference. The Command Line Interface (CLI) is the only interface available to administrators in the evaluated configuration. All of the configurable security functions are available through the CLI.

1.1 Purpose

This document has been developed to supplement information in the Trend Micro TippingPoint Threat Protection Command Line Interface Reference, so as to satisfy requirements for the content of administrative guidance described in Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5.

1.2 References

[ST] Trend Micro TippingPoint Threat Protection System v5.5.0 Security Target, Version 1.0, April 24, 2023

[CLI] Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, July 2021

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

[DG] Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, October 2021

1.3 Abbreviations

The following abbreviations are used in this document:

CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LSM	Local Security Manager
NIAP	National Information Assurance Partnership
PP	Protection Profile
RFC	Request for Comments
RHEL	Red Hat Enterprise Linux
SHA	Secure Hash Algorithm
SMS	Security Management System
SNMP	Simple Network Management Protocol
SSH	Secure Shell

TCP	Transmission Control Protocol
TSF	TOE Security Functions
TOE	Target of Evaluation
VM	Virtual Machine
vTPS	Trend Micro TippingPoint Threat Protection System virtual appliance model

2 Delivery and Secure Acceptance Procedures

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

2.1 Product Delivery

2.2.1 Hardware

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

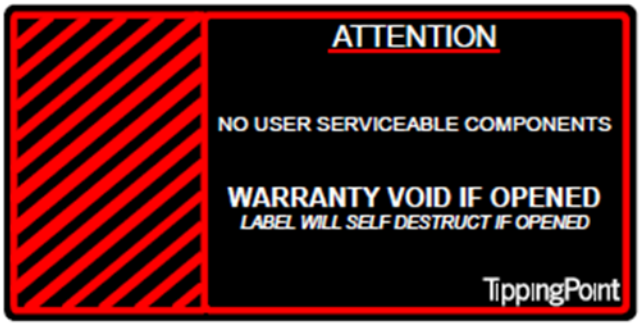

Figure 1: Example of Cover Security / Warranty Void Label

2.2 Software Downloads and Updates

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

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

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

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

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

2.3 Product Identification

The hardware is labeled externally with the hardware model number (example: TPNN0321). This number identifies the hardware model and can be matched by the customer against the label on the shipping box to verify that they have received the correct, certified hardware. The model number also references a bill of materials to ensure that the correct software release is pre-loaded onto the TOE before it is delivered.

2.4 Method of Packaging and Shipment

2.4.1 Packaging

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

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

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

2.4.2 Shipping

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

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

2.4.3 Tracking

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

2.5 Identification of Proper Delivery

The customer should check that their order of the TOE has been delivered in the correct version and part number as identified in the ST and in Section 3 below.

There are several mechanisms provided in the above process for a customer to ensure that they have received a product that has not been tampered with:

- Outside packaging—if the outside shipping box and tape have not been broken, and the outside shipping label properly identifies the customer and the product, then the product has not been tampered with.
- Inside packaging—if the plastic bag or seal on the plastic bag is damaged or removed, the device may have been tampered with.
- Tamper seals—if any tamper seals are broken or removed, the device or software may have been tampered with.

3 Configuration for Common Criteria

The following Trend Micro TippingPoint Threat Protection System devices running software version 5.5.0 (collectively, the Target of Evaluation or TOE) have been evaluated as satisfying the requirements specified in the ST:

- Trend Micro TippingPoint 1100TX (TPNN0321)
- Trend Micro TippingPoint 5500TX (TPNN0322)
- Trend Micro TippingPoint 8200TX (TPNN0090)
- Trend Micro TippingPoint 8400TX (TPNN0091)
- Trend Micro TippingPoint vTPS (VMware) (vTPS_vmw_5.5.0.2130.zip)
- Trend Micro TippingPoint vTPS (KVM) (vTPS_ kvm_5.5.0.2130.tar.gz)

The 1100TX includes one I/O module slot, the 5500TX includes two I/O module slots, and the 8200TX and the 8400TX include 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	TPNN0196/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 v5.5.0, running on hosts with Intel Haswell-based or Ivy Bridge-based microprocessors and either

- an ESXi Hypervisor: Version 6.7 or 7.0.2 (only paid versions supported), or
- a RHEL version 7.1 KVM.

The following table identifies the processors used in each of the hardware appliances.

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

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

To fully meet the requirements for evaluated Common Criteria certification, certain features must be configured in a specific way and the devices must be used within certain guidelines. In addition, certain features are not covered by the scope of the evaluation. This document describes Common Criteria configuration guidelines for the Trend Micro devices listed above.

The TPS requires a syslog server for external storage of audit data and an SSH client for remote administrative access to the CLI.

3.1 vTPS Virtual Appliance Installation

The vTPS virtual appliance must be the only guest running in the virtualized environment. The following provides the guidance to install the vTPS Virtual Appliance in the different virtual environments:

Refer to the following sections of [DG] for the guidance to deploy the vTPS appliance.

- ESXi – See Section “Install and deploy a vTPS virtual appliance by using VMware ESXi”
- KVM – See Section “Install and deploy a vTPS virtual appliance by using KVM”

3.2 Scope of Evaluation

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

- The TippingPoint Threat Protection System solution includes Local Security Management (LSM) and Security Management System (SMS) components that provides remote administrative management. In the evaluated configuration, all management must be performed using the CLI.
- The Digital Vaccine service is provided by the TOE developer and assumed to be a trusted

service. It may be used in the evaluated configuration, however it is not included in the TOE itself and therefore no claims are made about its ability to provide adequate or timely filter updates.

- The TPS devices can be configured to use sFlow record emission to sample a random flow of traffic and send the data to a collector server for analysis. SFlow and collector services are excluded from the evaluated configuration and must not be configured or used.
- Two TippingPoint Threat Protection appliances can be installed in a redundant network configuration. This system configuration provides High Availability (HA), ensuring that the network traffic always flows at wire speeds in the event of any internal hardware or software failure on the device. HA configurations are not covered in the scope of the evaluation.
- TippingPoint Threat Protection appliances can be installed in a stacking configuration. Stacking enables an organization to increase the overall inspection capacity of the TPS by grouping multiple TX Series devices and pooling their resources. Stacking configurations are not included in the evaluated configuration. The devices are being evaluated in a standalone configuration.
- Optional bypass I/O modules are available for the 1100TX, 5500TX, 8200TX, and 8400TX security devices that provide high availability for copper and fiber segments. These modules are not included in the TOE and must not be used in the evaluated configuration.

3.3 Operating Environment Objectives

The authorized administrators must ensure that the following operating environment objectives are met for Common Criteria operation:

- The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
- TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks..
- 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.
- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
- Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
- 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.

3.4 Configuring the TPS for Common Criteria Compliance

To ensure the TPS device is configured within the requirements of the evaluated configuration for Common Criteria, the following configuration actions must be taken:

- The TPS must be configured to support the Federal Information Processing Standards 140-2 (FIPS 140-2) cryptographic requirements. The *fips-mode-enable* command enables the Federal Information Processing Standard (FIPS) on a TPS device.

  Before you run this command, always reset the device to factory default settings. When you run this command, it prompts you to confirm that you want to enable FIPS mode. After you enable FIPS mode, it cannot be disabled except by resetting the device to factory defaults. After you run this command, you must reboot the device to enable FIPS mode. Use the *show fipsmode* command to verify FIPS mode is enabled.

FIPS Mode restricts the cryptographic mechanisms to FIPS-approved algorithms. See section 3.6.2 of this document for more information.

- During initial device configuration an administrative account is created with the default Super User role. The Super User role gives the account full access to the device. This administrative account is used to complete initial configuration. The password must be set prior to first use by the administrator performing the initial setup; there is no 'default' password that can be used to access the TOE. Guidance on choosing secure passwords is provided in Section 3.6.4 of this document. The Super User account itself must also be used to create other users and associate roles with roles. Other than super user, the default roles are: admin and operator. See Section 3.8 below for further details.
- The Trend Micro TPS and vTPS appliances must be deployed in a physically secure location to prevent physical tampering. Any person with physical access to the device must have the same level of trustworthiness as an authorized administrator.
- To manage a Trend Micro TPS and vTPS device in a way consistent with the evaluated configuration, device management must be performed via the CLI. Administrators manage the TOE remotely using an SSH connection to the Ethernet Management port on the TOE appliance or locally through the console interface or locally through a direct connection to the Ethernet Management port. Each method provides access to the CLI after an administrator successfully logs in. Prior to administrative login, the Management interface will respond to ICMP requests to confirm connectivity (for remote administrative connections) and displays a warning banner for both local and remote connections. No other TSF-mediated actions are permitted on behalf of an administrative user until the user is successfully authenticated. SSH access is enabled by default to allow CLI access to the device. No configuration is necessary. Non-secure access through Telnet is not permitted.

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

  Refer to the [CLI] command: *ips{running-aaa}user* to configure new users. You can create, modify, delete users and add or remove them to/from a user group on the local device database using *ips{running-aaa}user-group*. Access to the CLI is determined by the users' group membership and roles. Role determines a user's access to security functions. Authorization is controlled by granting users access through the authentication context (aaa).
- Telnet, and HTTP, and connections over untrusted networks are not supported and must not be enabled. Refer to the [CLI] for more details on using the CLI interface.

3.4.1 Setting the System Time/NTP

To set the system time on the Trend Micro TPS, use the command: *date [MMDDhhmm[[CC]YY][.ss]]*. This allows the following values to be set:

- Date

- Time.

Example: *ips{}date 071718202013.59* (sets date to July 17 2013 6:20PM 59 seconds).

Timezone is set using the command: *timezone (GMT|(REGION CITY)).*

The timezone command is found under the general context mode (gen): *ips{running-gen}timezone*.

To configure the TOE to sync its time with an NTP server, configure the remote NTP server using the command: *server (dhcp|A.B.C.D|X:X::X:X|FQDN) [key ID] [prefer].* The following values can be set:

server (dhcp|A.B.C.D|X:X::X:X|FQDN) [key ID] [prefer]

dhcp //Get server address from dhcp

or

NAME NTP remote server //enter the server name

Key ID //optional - specify a number between 1 and 65535 for the Key ID on the server.

prefer //Mark server as preferred (optional)

Example: *ips{running-ntp}server 192.158.1.38*

3.4.2 Configure the syslog server

In the evaluated configuration, TPS forwards generated audit records to an external syslog server as they are written to the local log files. To configure the syslog server, reference CLI Guide Section "To configure the "Remote System Log" contact to use SSH". It is expected that the syslog server need only be configured once. The SSH client key pair is generated by TPS as part of configuration during initial installation.

The following commands provide an example of the commands required to configure the Remote Syslog Export for a syslog server with IP address of 172.16.24 port 514.

```
vtpsESXi{running-notifycontacts-Remote System Log}display
#contact "Remote System Log" # syslog
  server 172.16.1.24 514
  alert-facility 172.16.1.24 514 4
  block-facility 172.16.1.24 514 4
  protocol 172.16.1.24 514 TCP
  ssh-user-name 172.16.1.24 514 <SERVER USER NAME>
  ssh-user-key 172.16.1.24 514 *****
  ssh-host-key 172.16.1.24 514 172.16.1.24 ssh-rsa <SERVER HOST KEY>
  use-ssh 172.16.1.24 514 enable
  period 1
  exit
```

The physical syslog server requires sshd (openssh 8.2p1) and rsyslog (8.2001.0) on an Ubuntu 20.04.3 machine.

3.5 Security Audit

3.5.1 Configuring Log Size/Rotation Settings

The TPS stores the audit records locally and can also 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 device's audit log (in real-time).

The TPS provides the ability to configure the size of the Audit and System logs. By default the total set of system logs and set of audit logs each take up half the available space. The term 'set' in this context means that if for example system log takes up 60% of the space and it has five backup files in a rotation, each backup and the main file will take up to 10% of the space each. And if audit also has five backup files and takes the other 40% of the space, each of those files will take up to 6.67%. As such these limits 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 log rotation function allows administrators to further control the amount of audit records that are stored. The current log is polled at a configurable interval to see if it has reached the maximum size. The administrator can specify the maximum size of a log file using the 'maxFileSize' parameter to configure how large a file can be (10MB – 500 MB) before rotation is triggered. They can specify the number of files kept in the log rotation (2 – 20) using the 'numfiles' parameter. Within each log file, they can also specify the maximum number of records contained in each file using the 'numrecords' parameter, which sets the number of records between log daemon size checks of 100- 65535). defaultCheckRecords sets the default number of records between log daemon size checks (100-65535), and 'sleepseconds' that determine the frequency with which the logs are checked for and whether rotation is necessary (after a certain period of time of 1 – 65535 seconds has elapsed).

The TPS does not provide an interface where a user can modify the audit records, thus it prevents modification to the audit records. There are no commands to delete individual audit records. Super Users can use the command: **clear log-file** to delete the locally stored Audit log and IPS data files. There are no interfaces to modify stored audit or IPS data.

Note that the command: *'ips{running-log}delete'* is not used to delete audit records but rather to remove a syslog server so that the device no longer sends audit records to it. The command does not affect locally stored audit records and generated audit events will still be logged locally.

The TPS 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 not configurable. The audit record can be viewed by issuing the command: *show log-file system*. A sample of the audit record can be seen in Table 3 – Sample Audit Records (FAU_STG.3/LocSpace).

3.6 Cryptographic Support

3.6.1 Cryptographic Self-Tests

The TPS runs software module integrity tests and cryptographic known answer self-tests during initial startup. When successfully run without errors, these tests demonstrate the correct operation of the TSF. If a self-test fails, the TOE enters an error state where a system recovery prompt is displayed. Contact a TippingPoint support representative for assistance. The TOE doesn't perform any cryptographic operations while in the error state. All data output from the TOE is inhibited when an error state exists.

3.6.2 SSH Configuration

The TPS is required to be configured into FIPS mode as described in Section 3.4 of this document. FIPS mode automatically configures the use of FIPS approved algorithms and key sizes as specified in the [ST]. No further configuration is required to ensure the use of FIPS approved algorithms.

TPS is not subject to any situations that could prevent or delay key destruction. TPS strictly conforms to the key destruction requirements as specified in the PP in Section 1.1 of this document and defined in the [ST].

In its evaluated configuration, TPS uses *CTR_DRBG (AES)*for random bit generation and the following algorithms:

- 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, AED_AES_128_GCM and AEAD_AES_256_GCM (implicit for aes*-gcm@openssh.com) as its MAC algorithms.

The following key exchange methods used in SSH are not configurable:

SSH Client

- *diffie-hellman-group14-sha1*,
- *ecdh-sha2-nistp256*,
- *ecdh-sha2-nistp384,and*
- *ecdh-sha2-nistp521*.

SSH Server

- *diffie-hellman-group14-sha1*
- *diffie-hellman-group15-sha512*
- *diffie-hellman-group16-sha512*

SSH ciphers can be viewed, and enabled or disabled using the following commands:

debug ssh ciphers <cipher-name> enable

debug ssh ciphers <cipher-name> disable

show key

To remain in the evaluated configuration only the ciphers/algorithms specified above may be enabled and less secure ciphers/algorithms must not be enabled.

Public Key and MAC algorithms can be changed by modifying the sshd config file as root. Note that in the CC Evaluated configuration, the “none” MAC algorithm is not allowed. There are no other configuration options.

3.6.3 Supported Authentication Methods

In the evaluated configuration, the device supports the following methods of administrator authentication:

- Local administrator accounts with local password-based authentication

- Local administrator accounts with public key-based authentication

SSH key-based authentication is dependent on administrative action and is specified on a per-user basis. See [CLI] Section *SSH configuration* 'To upload a user public key'. The following demonstrates an example SSH-PUBLIC-KEY being uploaded:

```
FIPS8400TX1311{running-aaa-user-CCroot}display
user CCroot
  password $password$
  ssh-public-key "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDyCjeqv0e5giUCzRVcWZPcUGhBHdiavkRcebF4HrtKut
5n7za2rWmZ16qOZZN4p8l54xUH2z2y5dtsdrewPcPkH8s9+kNkQTzjnHwarMLmaC7rYmZ2R7M1E5+WNQnTj+6xx25Ba5c3MoMJYHd
QurEMaPTX+QY4z53AefsrnfOoqIfioG1iSIAD6gZJTPN4uz9Lz40MX2fHCIELDDYtlgI8jiv9olNILVZWBiiK5OHCxtCp1znvfc3u
MBCzcrr35ycq9V2bmoVBtGndIegkhJbAmqaIVek0w01W5UvC81RYz4KVGMCBsbdSHwiCRRMC3YSsLB+qO6DtpDurkgZLKKt"
  exit
```

If the user is using a typical SSH client to log in to the device, they can choose to use a password or key-based authentication at the client side with the SSH options PasswordAuthentication or PreferredAuthentications. See https://man.openbsd.org/ssh_config.5#PasswordAuthentication.

3.6.4 Password Considerations

When password-based authentication is used, administrators need to ensure the passwords they use are suitably secure. Many organizations, as a matter of policy, specify minimum requirements for choosing and constructing user passwords and such policies should be adhered to. Additionally, or where site-specific policies are not defined, administrators should consider the following when choosing passwords:

- Ensure the password is not too short—a minimum of 8 characters is suggested
- Use a mix of upper and lower case alphabetic, numeric, and punctuation characters
- Avoid using dictionary words or words readily associated with you (e.g., name of spouse, pet or favorite sports team)
- Consider using a passphrase—a combination of words that is easy to remember but difficult for an attacker to guess.

The TPS devices support the ability to configure minimum password length and complexity settings. This is accomplished using the command: *ips{running-aaa} password quality (none|low|medium|high).* The password quality levels provide minimum password lengths of 1, 8 or 15 characters. A Password Security Level of None enforces a minimum password length of 1. A Password Security Level of Low or Medium both enforce a minimum password length of 8. A Password Security Level of high requires the passwords to be at least 15 characters. Passwords can be comprised of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", ",", ".", "/", "<", ">", "?". Single and double quotes, spaces or back slashes are not allowed. The password quality levels *none|low|medium|high* provide additional restrictions on password composition as follows. 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.

3.6.5 Authentication Failure Handling

The number of failed authentication attempts allowed before the device locks a privileged account is configurable as is the lock out value. Refer to the [CLI] *ips{running-aaa}login* command. 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 the local console. If an Administrator account is temporarily locked out and immediate access is required, an override may be provided by contacting Trend Micro support. The lockout override is a one-time credential provided by Trend Micro support based on the serial number of the device and a random salt.

3.7 TOE Access

3.7.1 Inactivity Timeout

The administrator is automatically logged out, if a login session is idle for more than the specified time. The maximum time (in minutes) without any activity on the CLI before an administrator is automatically logged out can be set to any integer value from one to 32000 using the command: *ips{running-aaa}login* command. See [CLI] for more details.

3.7.2 Access Banner

A login banner is text that is added to the login page so that administrators will see information they must know before they log in. The banner is configured using the command: ips{running-aaa}login-banner as described in "**Contexts and related commands**" section in the CLI Guide.

3.8 Security Management

3.8.1 Administrator Accounts and Roles

The TPS provides a predefined set of user groups that each have an assigned role with set access privileges. The permissions assigned to the default roles/groups cannot be modified. Each user group has an associated role that determines the type of administrative functions that are allowed.

The pre-defined default groups/roles are:

- Administrator – Has Read/Write privileges to all TPS capabilities except administering local users, user groups, and roles; and changing the password for other users.
- Operator – Has Read-only privileges to all TPS capabilities. Operator privileges are for a base-level administrator user who monitors the system and network traffic.
- Super User – Has Read/Write/Execute privileges to all TPS capabilities. Super User privileges include full access to all CLI functions. Only users associated with the Super User role can change the password for another user.

Administrators with the Super User role can create other users and assign them to administrator roles. The product also allows administrators with the Super User role to create, edit, and delete any user group except the default groups; however, this functionality was not tested in the evaluation.

The following table identifies the role an administrative user must have to manage the security functions.

Table 1 –Administrator Actions and Role Needed

Administrator Action	Role
Startup and shutdown of the audit function	Super User Admin
Configure Access Banner	Super User Admin
configure the session inactivity time before session termination or locking	Super User Admin
update the TOE, and to verify the update	Super User Admin
configure the authentication failure parameters for FIA_AFL.1 • unsuccessful authentication attempts • Lockout time period	Super User Admin
Configure audit behavior • Configure communication with external syslog • Configure log size/rotation • Clear local log files	Super User
configure the cryptographic functionality	Super User
Reset another user's password	Super User
Set time	Super User Admin
Create a local user	Super User
Management of password policy	Super User
Management of IPS Functions	Super User Admin

3.8.2 Revoking Administrator Privileges

The Security Administrator can revoke administrator privileges in either of the following ways:

- Deleting the user account entirely using the command: *ips{running-aaa}delete user (USER)*, or
- Removing the user from the administrator's group/role using the command: *ips{running-aaa-usergroup-GROUP}delete user USER*.

3.9 TOE Updates

The TPS 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. The integrity of the update is verified prior to installation using a digital signature. TippingPoint Technical Support releases software updates on the Threat Management Center (TMC): *https://tmc.tippingpoint.com*. Administrators with the Super

User role can download and install updates from this site. Installing a new software package forces a reboot of the device. Before performing an upgrade, the following should be considered:

- Refer to the TPS release notes for information specific to your TOS, including DV packages, migration, rollbacks, and traffic interruptions.
- To avoid experiencing traffic interruption whenever the operating system is rebooted, perform a full reboot of the device by running the reboot full command from the device CLI. This issue is not applicable to vTPS devices.
- On vTPS devices, the flow of traffic is interrupted during a TOS upgrade and during a reboot of the device.
- An upgrade resets the authentication settings on your TPS device. If the authentication security level on your device was set to Maximum, the upgrade resets the security level to Medium, which is the default security level. If necessary, update the security level to specify a higher security level. Learn more about authentication settings.
- Verify that a recent license package is installed on the device and if necessary, download and install a new license package from the TMC at https://tmc.tippingpoint.com. Without a recent license package, the device reverts to its unlicensed throughput.
- Maximize the space on your device by removing old TOS versions and packet traces. This ensures a successful installation and allows for a TOS rollback, if necessary. You can remove previous TOS versions by using the SMS, the LSM, or the CLI. For complete information, refer to your product documentation.

The command *show version* displays the current software version.

The administrator uses a Debug command (*debug upgrade URL*) to download a TOE update package directly from the 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 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.

If a TPS software update fails because of an invalid signature for example, an error report and a system log entry are generated. The device remains at its current version and configuration and the update is not performed. Customers are advised to contact Trend Micro support for assistance with these commands.

3.10 Intrusion Prevention System

The TOE's Threat Suppression Engine is a line-speed hardware engine that implements the Intrusion Prevention functions focusing on inspecting the IP traffic (TCP, UDP, ICMP, etc.). The TSE protects the network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device. This section provides an overview of the configurable IPS functions and the security management functions available from the CLI to manage the settings.

The TOE uses Digital Vaccine (DV) filters to police the network and to screen out malicious or unwanted traffic. In addition to the DV filters, the TOE also provides Traffic Management filters, which are custom filters that react to traffic based on source IP address, destination IP address, port, protocol, or other defined values. Traffic management filters are applied to traffic before DV filters. Each DV package has a unique ID that the DV distribution service uses to distinguish different DV packages. Each DV filter has a

Category, an Action set, and State and is customizable to be enabled or disabled and to identify an action set. The **Category** component defines the type of network protection provided by the filter (e.g. exploits, security-policy, spyware, virus). The category is also used to control the global filter settings using the Category Setting configuration. The filter categories can be enabled or disabled and action sets can be applied to the filters using the **category-settings** command. If a category is disabled, all filters in the category are disabled. When a filter is disabled, it is not applied to traffic. Limits and exceptions change the way filters are applied based on IP address. For example, a limit setting can be specified so that filters only apply to specific source and destination IP addresses or address ranges. If a filter has both global and filter level exception settings, the Threat Suppression Engine uses the filter-level settings to determine how to apply the filter. The following limit and exceptions can be configured:

- **Filter Exceptions** (specific) — Allow traffic that would normally trigger a filter to pass between specific addresses or address ranges without triggering the filter. Configured using the **Filter** command, these exceptions apply only to the filter where they were configured.
- **Limit Filter to IP Addresses** (global) — Only apply filters to traffic between specified source and destination IP address pairs. IP address limits can be configured that apply to Application Protection, Traffic Normalization, and Network Equipment Protection filter types. Separate limits can be configured that apply only to Performance Protection filters.
- **Exceptions** (global) — Exclude traffic between specified source and destination IP address pairs. Exceptions can be configured for the following filter types: Application Protection, Traffic Normalization, Network Equipment Protection, and Performance Protection filters. These exceptions are global for all specified filters.

Each filter also has an Adaptive Filter Configuration State component that allows the global Adaptive Filter configuration to be set to over-ride so that the filter is not affected by adaptive filtering. Adaptive filtering works by monitoring each filter to identify any suspected of causing congestion. When it identifies a filter, it manages the filter using one of the following methods, depending on how the global or filter-level Adaptive Filtering is configured:

- **Automatic Mode** — This setting enables the IPS device to automatically disable and generate a system message regarding the defective filter.
- **Manual** — This setting enables the IPS device to generate a system message regarding the defective filter. However, the filter is not disabled.

The following IPS management configurations are also available:

- Modify the duration of traffic blocking actions: Edit >>ips >>connection-table
- Configure the known-good and known-bad lists to override signature-based IPS policies
    - Edit>>ips>>profile "profile name" >>exception (for policy level exceptions)
    - Edit>>ips>>profile "profile name" >>filter " filter number" >>exception (for signature based exceptions)

A security profile defines the traffic that the IPS monitors and the signature-based DV filters that the IPS applies. Traffic monitoring is based on incoming and outgoing port pairs. The administrator can use the default DV filter configuration to protect the segment or customize the configuration as required. The segment specifies both the port and the traffic direction, which allows definition of separate security profiles for traffic in and out of a port. Traffic management filters are configured in the context of a traffic management profile that determines which network segments are monitored by the filter. The Traffic management profile defines IP layer parameter configuration to control packet flows. If a security profile is not specified for the filter, the filter is applied to the Default security profile.

The default security profile is set to ANY incoming ports and ANY outgoing ports, with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic on any virtual segment configured on the device is monitored according to the IPS filter configuration recommended by TippingPoint. The administrator can customize the default security profile with the virtual segments that it applies to, modify the filter settings, or modify the security profiles as required. The **profile** command can be sued to create, modify, or delete security or traffic management profiles. The subcommand **traffic-mgmt** can be used to create a traffic management profile.

Anomaly-Based IPS Functionality:

The TOE supports anomaly traffic patterns for inline traffic by providing the ability to define rate-limit policy filters that specify throughput thresholds in Kbps that can be applied to the traffic. The thresholds define the frequency at which traffic (in kilobytes) can traverse the TOE (per second) before the filter is triggered. Traffic that deviates from the defined throughput thresholds is considered unexpected or atypical and treated as potentially malicious. Filters for anomaly-based policies can be applied to any of the network protocol fields (all packet header and data elements defined in IPS_SBD_EXT.1. Each rule can be associated with any of the following operations for inline traffic using the **action-set** command:

- allow the traffic flow
- block/drop the traffic flow
- send a TCP reset to the source address of the offending traffic;
- send a TCP reset to the destination address of the offending traffic;
- send an ICMP (host, destination, port) unreachable message.

Rate-limit policy filters are defined in traffic management profiles using the **rate-limit** subcommand to create/modify an action (as defined above) that rate-limits traffic according to the identified threshold (defined in Kbps). Traffic matching a rate-limit filter is subsequently inspected based on the security profile configuration (DV filtering). That is, traffic is not allowed through the device based solely on the rate-limit traffic management filter criteria. Rate-limit policy filters rules can be applied and enforced on any of the TOE's sensor interfaces. Different TPS appliances support different sensor interfaces ranging from 1GbE to 40GbE.

DV filters are included in the system as the place-holder for users to define the frequency and threshold values identified above as used in anomaly-based detection and prevention.

Traffic matching the manually configured anomaly-based rules (rate-limit) are subsequently inspected based on the security profile configuration (DV filtering).

IP Blocking:

The TOE supports configuration and implementation of known-good and known-bad lists of source and destination IP addresses. Configuration of the policy elements is restricted to the IPS Administrators (i.e. users with the Super User or Admin role). Known-bad lists are configured and provided through traffic management filters. Known-bad lists and additionally known-good lists can be configured in Reputation filters within a Security Policy using the **reputation** and **reputation groups** commands that allows an administrator to create groups of IPv4, IPv6, and DNS addresses, and apply block, permit, or notify actions across an entire reputation group. After a group is configured, security profiles can be configured to apply reputation filters to the group. Additional inspection is performed after Reputation checks by the DV Filters. Overrides to the additional signature based policy inspection can be implemented from the console >>Edit>>IPS>>profile "profilename" >>filter "filter number" >>Exception.

When an IP address or DNS name is added to a reputation group, it is added to the device's reputation database. Incoming traffic is checked against the database, and the appropriate reputation filters are then

applied. Traffic management filters are configured in the context of a traffic management profile that determines which network segments are monitored by the filter. If a security profile is not specified for the filter, the filter is applied to the Default security profile.

The TOE provides the Reputation ThreatDV package that is separate from the standard DV filter package. This package includes pre-defined known-bad lists. Reputation ThreatDV package updates can be obtained in the same manner as the standard DV packages as described below under Signature-Based IPS Functionality.

Network Traffic Analysis:

The TOE performs analysis of IP-based network traffic forwarded to the TOE's sensor interfaces, and detects violations of administratively-defined IPS policies. The TOE is able inspect and process the following network protocols: IPv4 (RFC 791); IPv6 (RFC 2460); ICMPv4 (RFC 792); ICMPv6 (RFC 2463); TCP (RFC 793); and UDP (RFC 768). Trend Micro determines protocol conformance through developer testing in the context of filter behavior.

The TOE provides approximately 20,000 filters that are the basis for its signature-based IPS functionality. Not all filters are turned on simultaneously. Some filters apply to perimeter TPS devices while others are for interior TPS devices. The TOE provides pre-packaged profiles (for example standard, aggressive, hyper-aggressive). Each pre-packaged profile balances filtering and false policy. New filters are published on a regular basis and customers are provided with descriptions and guidance for the new filters. Filters are preset to on or off in filter profiles, but an administrator can enable/disable as needed. The filter profiles (containing signatures) can be assigned to the TOE's sensor interfaces configured for inline mode (1, 10, 40 GB Ethernet data interfaces, virtio or vmxnet3 for vTPS) and supports designation of both a 1 Gb Ethernet (SSH access to CLI) and a serial interface (CLI) as management modes for communication between the TOE and external entities without simultaneously being sensor interfaces. Promiscuous mode is not supported.

The TOE's policy hierarchy (precedence) is as follows: reputation filters are applied between anomaly-based filters and signature-based filters. The order of these filter matching operations cannot be changed except for signature-based filters, which have a pre-defined precedence; all other types of filters are applied in the order of their definition.

Signature-Based IPS Functionality:

Trend Micro provides approximately 20,000 filters. Not all filters are turned on simultaneously. Some filters apply to perimeter TOE devices while others are for interior TPS devices. Trend Micro provides pre-packaged profiles (for example: standard, aggressive, hyper-aggressive). Trend Micro publishes new filters to their Threat Management Center (TMC) on a regular basis and sends descriptions and guidance for the new filters to customers. Filters are preset to on or off in filter profiles, but an administrator can enable/disable as needed. Filters can be applied by interface. The command **conf t autodv** enables and disables the automatic download service for Digital Vaccine updates. This command requires a day of week and time of day for the download. If desired, the administrator can use the **-period** option to set the number of days between checks.

A string-based detection signature or rule is comprised of the string or the attack's signature to be matched with the packet's payload. The TOE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination.

Additional details about the configurable IPS functions and the security management functions available can be found in the CLI reference guide.