Virtual Threat Protection System Functional Differences Addendum

Version 4.2.0

March 2017

Legal and notice information

Trend Micro makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

TippingPoint Virtual Threat Protection System Functional Differences Addendum

Contents

About this guide

The Virtual Threat Protection System (vTPS) is a software appliance designed to give you the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically.

This version of the vTPS supports the majority of features that are included with the corresponding version of physical TPS devices. This guide describes the configuration differences and other special considerations for deploying a TPS in a virtual environment.

This section covers the following topics:

- *Target audience* on page 1
- *Conventions* on page 2
- *Product support* on page 3

Target audience

This guide is intended for security network administrators and specialists that have the responsibility of monitoring, managing, and improving system security. The audience for this material is expected to be familiar with the TippingPoint security systems and associated devices.

Users should be familiar with the following concepts:

- Basic networking
- Network security
- Routing

Related documentation

The vTPS product uses the same documents set for a physical TPS, including user guides, CLI command references, and safety and compliance information.

In addition to the product documentation set associated with a physical TPS device, the following content is provided specifically for vTPS users:

- This functional differences addendum
- A *Virtual Threat Protection System Deployment Guide* that provides configuration options and other special considerations for deploying a TPS in a virtual environment
- Release notes that describe changes and new features included in this release

A complete set of product documentation for your TippingPoint security device is available on the TippingPoint Threat Management Center (TMC) at: *https://tmc.tippingpoint.com*.

Conventions

This information uses the following conventions.

Typefaces

TippingPoint uses the following typographic conventions for structuring information.

Convention	Element
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click **OK** to accept.
Italics font	Text emphasis, important terms, variables, and publication titles
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

Messages are special text that is emphasized by font, format, and icons.

⚠**Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

△**Caution:** Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

Note: Provides additional information to explain a concept or complete a task.

Important: Provides significant information or specific instructions.

Tip: Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Product support

Get support for your product by using any of the following options:

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

vTPS functionality

The Virtual Threat Protection System (vTPS) is a software-based security device that can inspect traffic in a virtual network between Layer 2 broadcast domains. With few exceptions, the vTPS platform is designed to be functionally identical to a physical TPS device.

The vTPS has most of the same features as the TPS device, including:

- HTTP response processing to decode URL encodings and numeric character references
- DNS reputation remediation for enabling `NXDOMAIN (name does not exist)` responses to clients that make DNS requests for hosts that are blocked
- Layer 2 Fallback (Intrinsic High Availability)
- Enhanced SNMP support
- The ability to collect a client's true IP address.
- The ability to identify the HTTP URI and hostname information associated with an event.
- Flexibility to upgrade inspection throughput from 500Mbps to 1Gbps.

For successful TPS functionality in a virtual environment, the vTPS:

- Supports Layer 2 IPS deployments—The vTPS connects the virtual switches. Traffic between the virtual switches is bridged on these connections using promiscuous mode.
- Provides full protection of North-South traffic.
- Provides limited protection of East-West traffic (according to existing network policy constructs).

For optimal deployment of your vTPS, you should note the specific areas in which your virtual device functionality differs from a physical TPS device.

Note: With the exception of VLAN Translation, any unsupported features will not be displayed in the three vTPS interfaces—Local Security Manager (LSM), command-line interface (CLI), and Security Management System (SMS).

The following topics highlight the areas where a vTPS device diverges functionally from a physical TPS device:

- *Deployment and licensing* on page 5
- *Specifications* on page 6
- *Unsupported features* on page 8
- *LSM user interface* on page 8
- *Commands* on page 9

Deployment and licensing

Because the vTPS is a virtual product, the out-of-box experience (OBE) for vTPS users is provided by way of an email from TippingPoint. This email contains the necessary licensing and activation information. For details on deploying a vTPS device, refer to the *Virtual Threat Protection System Deployment Guide*.

When setting up your vTPS device, note the following:

- The vTPS initially starts up in vTPS Trial Mode. Trial Mode is primarily exploratory and comes with a limited number of security filters in the Digital Vaccine (DV) package. In this mode, an SMS can manage only one vTPS at a time. Because Trial Mode has a fixed serial number and entitlement, you cannot use Trial Mode to perform TippingPoint Operating System (TOS) upgrades or distribute DVs.
- After logging in to their systems, users can upload their certificates for a vTPS Standard deployment from the TippingPoint entitlement system. The vTPS device remains in Trial Mode until a valid certificate for vTPS Standard is loaded. For information on upgrading to vTPS Standard Mode, refer to the *Virtual Threat Protection System Deployment Guide*.

  Note: If the vTPS will be managed by an SMS, users must first add the device to the SMS so that the device certificate and UUID is available to the SMS.

- The device (or the SMS) prompts users to reboot, at which point the new certificate is loaded on the device and users can connect to the TMC with an active license. From the TMC, users download the Entitlement package for a vTPS Standard deployment. The package contains:
  - Digital Vaccine (DV) and ThreatDV packages
  - Licensing information for the device
  - Inspection capacity associated with the vTPS instance
- The vTPS Standard serial number can be retrieved from the license certificate.

The following table highlights the ways in which getting set up on a TPS and vTPS are different:

Deployment	TPS	VTPS
OBE	After you install the device in a rack, a setup wizard guides you through system checks, initializations, and configurations.	You open an email with activation and licensing information. Initial deployment defaults to a Trial Mode. No updates can be performed.

Deployment	TPS	VTPS
Digital Vaccine	Uses the V. 3.2.0.x DV package. This package is encrypted with an IPM chip.	Uses a special DV package (4.0.0.*x*) that does not include Zero Day Initiative (ZDI) filters. This package is encrypted with an RSA key embedded in the software.

Authentication	Local users are members of LDAP groups or RADIUS groups.	Local users can be assigned SSH public keys to log in to their accounts without a password. Configure this through the LSM or the CLI.
		CLI:
		`ipsdev{}edit`
		`ipsdev{running}aaa`
		`ipsdev{running-aaa}user USERNAME`
		`ipsdev{running-aaa-user-USERNAME}`
		`     ssh-public-key [PUBLIC KEY OF USER]`
		LSM:
		1. Navigate to **Authentication > Local Users**.
		2. Click **Add** to create a new local user or **Edit** to change an existing one.
		3. Enter the SSH public key in the SSH Public Key field.

Specifications

Both the TPS device and the vTPS Standard device (including a vTPS deployed in Trial Mode) have the following common specifications.

Description	Specification
IPS inspection throughput	Two-core vTPS: 500 Mbps Three-core vTPS (upgrade license required): 1Gbps
Average IPS latency	Less than 100 microseconds
Security contexts	750,000

The specifications of the physical TPS device and the vTPS Standard device differ in the following areas.

Description	TPS	vTPS
Concurrent sessions	440T: 7,500,000 2200T: 10,000,000	1,000,000
New connections per second	440T: 70,000 2200T: 115,000	VMware: Up to 120,000 KVM: Up to 60,000

The following functionality is different in the vTPS Standard device.

Specification	TPS	vTPS Standard
Port configuration	Eight data ports. Physical characteristics of ports (such as speed and duplicity) can be configured. Ports are fixed.	Two virtual data ports. Physical characteristics of ports (such as speed and duplicity) cannot be configured. A port can be removed and replaced.
User disk	External 8GB CFast card.	No separate user disk. The vTPS Standard device has a single-disk architecture with a user disk partition.
Environmental requirements	For operating, storage, and environmental requirements, refer to the *Threat Protection System Hardware Specification and Installation Guide*.	Not applicable.
External HA interfaces	1 HA port 1 ZPHA port	No HA ports supported.

Unsupported features

All available features can be configured using the vTPS interfaces (LSM, CLI, SMS). With the exception of VLAN Translation, any unsupported features will not be displayed in the LSM, CLI, or SMS.

The following features that are supported in the physical TPS are not supported in the vTPS Standard device:

- Physical characteristics of ports (such as speed and duplicity). Ports are virtual instead of copper or fiber.
- Data security (configuring the system master key and encrypting the removable disk that stores logs)
- Link setting updates when you configure a port
- High Availability deployments
- VLAN Translation
- East-West protocol (such as VXLAN)

LSM user interface

The following Local Security manager (LSM) options for a physical TPS device are not available on the vTPS. With the exception of VLAN Translation, any unsupported options are not displayed in the LSM.

Operation	Explanation
Monitor > Health > HA	The vTPS device does not support high availability deployments.
Monitor > Health > Fan Speed	Environmental and operational constraints are not applicable.
Monitor > Health > Temperature	Environmental and operational constraints are not applicable.
Network > VLAN Translations	Although this menu option will still be displayed, VLAN translations are not supported.
Network > Ports > Settings page.	When you use the **Edit** button, you can configure only whether the port is enabled or not.

Operation	Explanation
Policy > Inspection Bypass	The vTPS device does not support high availability deployments.
System > Data Security	There is no external storage card on a virtual device. The size of the user disk has no restrictions.
System > High Availability	High availability deployments are not supported.

Commands

The following commands that are supported when you use a physical TPS device are not available for the vTPS:

- Data security
  - `log-storage`
  - `master-key (clear|get|set)`
- Health
  - `reports (reset|enable|disable) fan`
  - `reports (reset|enable|disable) temperature`
- Port settings
  - `interface ethernetx physical-media`
  - `interface mgmt ip-filter`
  - `interface mgmt ipaddress`
  - `interface mgmt physical-media`
  - `bind in-port PHYSPORT out-port PHYSPORT`
  - `delete bind in-port EXISTING_PHYSPORT out-port EXISTING_PHYSPORT`
- High availability – You can use the following high-availability commands, but *only* for Layer2 Fallback settings:
  - `high-availability`
  - `edit high-availability`

    - `show high-availability`