Virtual Threat Protection System (vTPS) Functional Differences Addendum

October 2017

Legal and notice information

Virtual Threat Protection System (vTPS) 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

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
- Virtualization

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

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

The following typographic conventions for structuring information are used.

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

Information for you to contact product support is available on the TMC at *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:

- In-line, real-time threat protection for inbound IPv4 traffic that is SSL encrypted (Performance image only)
- 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 500 Mbps to 1 Gbps.

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: 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

Because the vTPS is a virtual product, the out-of-box experience (OBE) for vTPS users is described in an email from Trend Micro TippingPoint. This email contains licensing and activation information and directs you to use the license manager on the TMC to create and download vTPS certificate packages. 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.
- The vTPS device remains in Trial Mode until a valid certificate for vTPS Standard Mode is installed. For information on upgrading to vTPS Standard Mode, refer to the *Virtual Threat Protection System Deployment Guide*.

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.	Obtain the license entitlement and certificate using the license manager on the TMC. Initial deployment defaults to a Trial Mode. No updates can be performed.
Digital Vaccine	Uses the V. 3.2.0.x DV package.	Uses a special DV package (4.0.0.*x*) that does not include Zero Day Initiative (ZDI) filters.

Specifications

Both the TPS device and the vTPS Standard device have the following common specifications.

Table 1. Performance numbers shared between TPS and vTPS

Description	Specification
IPS inspection throughput	100 Mbps (default) Up to 1 Gbps (upgrade license required)
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.

Table 2. Performance numbers that differ between TPS and vTPS

Description	TPS	vTPS
Concurrent sessions	440T: 7,500,000 2200T: 10,000,000 8200TX/8400TX: 120,000,000	1,000,000
New connections per second	440T: 70,000 2200T: 115,000 8200TX/8400TX: 650,000	VMware: Up to 120,000 KVM: Up to 60,000

Note: All virtual machines (VMs) on a shared host compete for resources. To achieve optimal performance numbers for the vTPS, ensure that the hypervisor provides adequate CPU and RAM for the VM. Performance numbers will vary depending on hypervisor configuration and hardware resources available.

The SSL performance of the physical TPS device and the vTPS Standard device (must have Performance image deployed) differ in the following areas.

Note: The TPS 440T device does not support SSL inspection.

Table 3. SSL performance differences between TPS and vTPS

Description	TPS	vTPS
Profiles	8096	756
Policies	8096	756
Policy IP Exceptions	1024	128
Servers	1024	128
Server IPs	8	8
Server Ports	8	8
Certificates	2200T: 256 8200TX/8400TX: 256	32

The following functionality is different in the vTPS Standard device.

Table 4. Functionality differences between TPS and vTPS

Specification	TPS	vTPS Standard
Port configuration	Eight data ports. Physical characteristics of ports (such as speed and duplex) can be configured. Ports are fixed.	Two virtual data ports. Physical characteristics of ports (such as speed and duplex) cannot be configured. A port can be removed and replaced.
User disk	External 8 GB CFast card. (440T/2200T)	No separate user disk. The vTPS Standard device has a single-disk architecture with an 8-GB user disk partition.

Specification	TPS	vTPS Standard
	External 32 GB SSD (8200TX/8400TX)	
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). 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 duplex). Ports are virtual instead of copper or fiber.
- Data security (encrypting the removable disk that stores logs)
- Link setting updates when you configure a port
- Transparent High Availability (TRHA) deployments
- Zero Power High Availability (ZPHA) deployments
- VLAN Translation
- Inspection bypass
- sFlow® sampling
- Jumbo frames
- East-West protocol (such as VXLAN)
- Direct-attach network interface controller (NIC)

LSM user interface

The following Local Security manager (LSM) options for a physical TPS device are not available on the vTPS. 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	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.
Network > sFlow	The hardware required to run this feature is not available on vTPS devices.
Policy > Inspection Bypass	The Broadcom switch chip required to run this feature is not available on vTPS devices.
System > Data Security	There is no external storage card on a virtual device. Although users can provide a master key, the external storage card cannot be encrypted.
System > High Availability	Transparent High Availability (TRHA) and Zero Power High Availability (ZPHA) deployments cannot be configured on this page.

Commands

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

- Data security
  - `log-storage`
- Health
  - `reports (reset|enable|disable) fan`
  - `reports (reset|enable|disable) temperature`
- Port settings
  - `interface <port_identifier> physical-media`
  - `interface mgmt physical-media`
- High availability – You can use the following high-availability commands, but *only* for Layer2 Fallback settings:
  - `high-availability`
  - `high-availability force (normal | fallback)`
  - `show high-availability`
- sFlow sampling
  - `sflow`
  - `show sflow`
- Inspection bypass
  - `running-inspection-bypass` context commands
  - `show inspection-bypass`
- VLAN translation
  - `running-vlan-translations` context commands
  - `show vlan-translations`
- SSL inspection – You can use the `running-sslinsp` context commands, but *only* if a Performance image is deployed.