TippingPoint™

Virtual Threat Protection System (vTPS)

Functional Differences Addendum

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

Publication: July 2018

vTPS functionality

The Virtual Threat Protection System (vTPS) virtual appliance is a software-based security appliance 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 virtual appliance 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 mode 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 virtual appliance:

- Supports Layer 2 IPS deployments—The vTPS virtual appliance 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 virtual appliance, you should note the specific areas in which your virtual appliance 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 virtual appliance diverges functionally from a physical TPS device:

- *Deployment and licensing*
- *Specifications*
- *Unsupported features*
- *LSM user interface*
- *Commands*

Deployment and licensing

Because the vTPS virtual appliance 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 Threat Management Center (TMC) to create and download vTPS certificate packages. For details on deploying a vTPS virtual appliance, refer to the *Virtual Threat Protection System Deployment Guide*.

When setting up your vTPS virtual appliance, note the following:

- The vTPS virtual appliance 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 virtual appliance 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 virtual appliance remains in Trial Mode until you install a valid certificate for vTPS Standard Mode. For information on upgrading to vTPS Standard Mode, refer to the *Virtual Threat Protection System Deployment Guide*.
- The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

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

DEPLOYMENT	TPS DEVICE	vTPS VIRTUAL APPLIANCE
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. You cannot perform any updates.
DV	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 virtual appliance share the following specifications.

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 virtual appliance differ in the following areas.

DESCRIPTION	TPS DEVICE	vTPS VIRTUAL APPLIANCE
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
Ethernet maximum transmission units (MTU)	9050	1500

Note

All virtual machines (VMs) on a shared host compete for resources. To achieve optimal performance numbers for the vTPS virtual appliance, 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 virtual appliance (must have Performance mode deployed) differ in the following areas.

Note

The TPS 440T device does not support SSL inspection.

Description	TPS device	vTPS virtual appliance
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 virtual appliance.

Specification	TPS device	vTPS Standard virtual appliance
Port configuration	Eight data ports. You can configure physical characteristics of ports (such as speed and duplex). Ports are fixed.	Two virtual data ports. You cannot configure physical characteristics of ports (such as speed and duplex). You can remove and replace a port.
User disk	External 8 GB CFast card. (440T/ 2200T) External 32 GB SSD (8200TX/8400TX)	No separate user disk. The vTPS Standard virtual appliance has a single-disk architecture with an 8-GB 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

You can configure all available features using the vTPS interfaces (LSM, CLI, SMS). Any unsupported features will not be displayed in these interfaces.

The following features supported in the physical TPS devices are not supported in the vTPS Standard virtual appliance:

- 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

Note

This means that the vTPS virtual appliance does not pass traffic at all during a software upgrade or during a reboot of the device.

- VLAN Translation
- Inspection bypass
- sFlow® sampling
- Jumbo frames
- Reputation Enforcement Options (SMS-managed vTPS virtual appliance deployed in Normal Mode only)
- East-West protocol (such as VXLAN)
- Direct-attach network interface controller (NIC)

LSM user interface

The following LSM options for a physical TPS device are not available on the vTPS virtual appliance. Any unsupported options are not displayed in the LSM.

Operation	Explanation
Monitor > Health > HA	The vTPS virtual appliance does not support high availability deployments.
Monitor > Health > Fan Speed	Environmental and operational constraints do not apply.
Monitor > Health > Temperature	Environmental and operational constraints do not apply.
Network > VLAN Translations	VLAN translations are not supported.
Network > Ports > Settings page.	When you use the **Edit** button, you can only enable or disable the port.
Network > sFlow	The hardware required to run this feature is not available on vTPS virtual appliances.
Policy > Inspection Bypass	The Broadcom switch chip required to run this feature is not available on vTPS virtual appliances.
System > Data Security	vTPS virtual appliances do not have an external storage card. 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 a physical TPS device supports are not available for the vTPS virtual appliance:

- 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 Layer 2 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 you deploy in Performance mode.