Threat Protection System
Release Notes

Version 5.3.1

To ensure that you have the latest versions of product documentation, visit the Online Help Center.

Important notes

This release is supported on vTPS, 440T, 2200T, 1100TX, 5500TX, 8200TX, and 8400TX devices.

- If you are upgrading from an earlier, nonsequential TOS, refer to the release notes of any interim releases for additional enhancements.
- All TPS devices must be running a minimum of v5.0.1 before installing this version. Learn more.
- Use SMS v5.3.0 and later to manage a TPS device with this release.
- TippingPoint recommends any users requiring SSL Inspection to upgrade to this release.

Release Contents

Description	Reference
This release addresses a critical issue where SSL Inspection caused the device to enter Layer 2 Fallback.	TIP-46878 TIP-46877 TIP-46899 TIP-49714 TIP-49735
Rare conditions could prevent users from logging back in after a system crash without entering recovery mode.	TIP-50225
This release repairs an FPGA issue that failed to scrub abandoned network connections, which caused the FPGA connection table to become congested. The performance of 8200TX and 8400TX devices became degraded, and a reboot was required to recover from the condition.	TIP-47474
A condition that caused system clock adjustments to display invalid debug np tier-stats values has been resolved.	SEG-48804
The Tier 2 stats (Ratio to next tier) now correctly display the Tier 1 stats.	TIP-52853
When SSL operations reach a specific memory consumption threshold, SSL connections can now temporarily bypass the SSL proxy (and SSL inspection) until more memory is available.	TIP-51811

Known issues

Description	Reference
When you insert a 40 Gbps bypass module (BIOM) into a TX-Series TPS device that has not been upgraded to at least TOS v5.2.0, the module health status LED indicates that the module has experienced a fault (solid amber). To recover from this state: 1. Upgrade the device to TOS v5.2.0 or later. 2. After the upgrade, perform a full reboot of the device. 3. Disable bypass on all BIOMs by selecting the normal option: • SMS: From the Device menu, click the device and select **Device Configuration -> HA (High Availability) -> Zero Power HA**. • LSM: Select **System -> High Availability -> Zero-Power HA**. • CLI: `high-availability zero-power (bypass|normal) (slot|all)`	TIP-33655
Performing any kind of inspection, including SSL inspection, on VXLAN packets with a vlan tag in the outer (tunnel) header is not supported on 8200TX and 8400TX devices.	TIP-45595 TIP-45678

For optimal performance of URL filtering and other memory intensive features running on a vTPS in Normal mode, configure 16 GB of RAM.	TIP-33876
When you create a snapshot using the LSM, the browser sometimes times out even though the snapshot creation eventually succeeds.	TIP-37112
System logs do not indicate when the state of a transceiver changes.	TIP-39167
SSL inspection no longer supports compression within TLS/SSL, nor periodic rekeying.	TIP-32066
Because of an issue with HTTP Response Processing, do not change the default setting for encoded HTTP responses. From the LSM, select **Policy > Settings** and ensure that **Accelerated inspection of encoded HTTP responses** is selected.	TIP-49369
Under rare conditions, the following error can occur during DNS Reputation filtering: `Error TOSPORT NP: <thread> DNS Decoder: Parse of generated NXDOMAIN PDU failed; disposition is npDispositionEthTypeUnknown` The error indicates merely that the NXDOMAIN response packet was not sent back to the DNS requester. You can safely ignore the error message.	TIP-39422

Product support

For assistance, contact the *Technical Assistance Center (TAC)*.