Threat Protection System Release Notes

Version 5.3.2

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 v5.3.0 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 repairs an SMB flow issue in which Trust actions were slow to complete on 8200TX and 8400TX devices.	TIP-56512
Attempts to contact the peer device during TRHA no longer cause the system to freeze.	TIP-56762
Statistics from the following commands are now included in TSRs to help diagnose SSL issues: • `show ssl-inspection congestion` – includes the average number of SSL connections per second, the number of current SSL connections (and the device limit), and whether SSL sessions that exceed the device limit are not inspected or blocked. • `show system statistics fast-path`	TIP-56125
SSL connections that were not closed properly and did not give any notification would persist indefinitely. With this release, the connection will be dropped after a specified interval (60 seconds is the default). To configure this interval, contact TippingPoint product support.	TIP-56189
A stability issue in HTTP Response Processing has been repaired.	TIP-56954
Idle SSL connections can now be identified, reported and cleared out. This prevents increasing concurrent connections that are not really being used. If an `SSL Inspection reached Critical threshold` message is displayed in the system log, and users cannot modify their topology or application to close connections more reliably, they can contact TippingPoint product support to enable this SSL proxy idle timeout feature, which is disabled by default.	TIP-56250

Known issues

Description	Reference
Because congestion visibility is enabled by default, if you had it disabled in v5.3.1, you must manually disable it again after an upgrade to v5.3.2.	TIP-56634
In some rare cases, link-down synchronization can cause both sides of a segment to remain down or cause a port to be up when it should be down. You can rectify these situations by restarting the device and the ports.	TIP-57408

An issue exists that leads to the incomplete evaluation of certain application filters within the 8x00TX platforms. This issue manifests itself when application filters are activated within a policy set, with any flow control action (block, trust, rate limit). When the filter is incorrectly evaluated the defined action is not taken and notifications are not sent. No security filters are affected by this issue. Refer to Product Bulletin #1087 for more information, a list of affected filters, and mitigation steps.	SEG-102022

Product support

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