Threat Protection System Release Notes

Version 5.5

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 v5.4.0 before installing this version. Learn more.
- Use SMS v5.5 and later to manage a TPS device with this release. SMS v5.5 upgrades are only supported from an SMS installed with SMS v5.3.0. Attempts to upgrade from an older release will return an error. If the error message is blank, check the SMS system log for the complete message.

Release Contents

Description	Reference
The network performance of SMB and TLS (non-decrypted) traffic has been improved. Contact support prior to removing manual traffic bypass actions to ensure that ongoing performance needs are met.	TIP-50715

You can now configure your device to send notifications when it crosses a performance threshold so you can proactively monitor usage and address issues before they impact users.
You can monitor the current throughput utilization, the maximum values of the current throughput usage, and the actual licensed throughput with this new command:
`show np throughput-utilization`
You can clear the maximum values of the current throughput usage with this new command:
`clear np throughput-utilization-max`
Learn more about these commands in the *Command Line Interface Reference*.
	TIP-56177

The **TPT-NPSTATS-MIB** has been updated to include five new objects for throughput usage information, including: ▪ Current throughput ▪ Current percentage of licensed throughput ▪ Licensed throughput ▪ Highest throughput level reach since the last clear or reboot ▪ Maximum seen percentage of the licensed throughput since the last clear or reboot Learn more in the *Threat Protection System MIBs Guide*.	TIP-35469
An issue in which interprocess communications related to health statistics resulted in errors in some rare cases has been fixed in this release.	TIP-49034
Browser support for the LSM no longer includes Netscape. Users who are using Internet Explorer should transition to Microsoft Edge before Internet Explorer is retired on June 15, 2022.	SEG-113378
An OpenSSL vulnerability (CVE-2021-3449) that caused TPS appliances to enter Layer-2 Fallback (L2FB) mode and stop inspecting network traffic has been repaired in this release. To learn more, refer to the security bulletin.	TIP-64383
An issue affecting 8x00TX platforms has been corrected in which application filters were not completely evaluated. This caused the defined action to not be taken or notifications to not be sent.	TIP-62730

This release fixes an upgrade issue that caused the FPGA to enter into a fallback state with error code `0x8002`.	SEG-120772 SEG-88830
Devices no longer fail to communicate after a reboot.	SEG-118091
A group of `debug np` commands are now available as corresponding `show` commands (described below) to allow a device user with operator privileges to execute these commands (debug commands require superuser privileges). show np congestion — Show congestion breakdown show np diagx — Show low level network processor counters detail — Show more detail drops — Show more detail including per-port drops show np stats show fqStats — Flow queue statistics dpk — Data plane statistics npTcpReas dpk — TCP reassembly statistics show np regex-stats — Show regular expression statistics show np regex show count — Maximum number of entries to show (default 10) maximum — Sort by maximum time (default) average — Sort by average time evaluations — Maximum number of entries to show (default 10) matches — Sort by number of matches total — Sort by total time	TIP-57260
This release resolves a `Maximum number of packet captures have been reached` error that occurred when TCP Dump processes remained active after the completion of a packet capture.	SEG-102664

Known issues

Description	Reference
Performing a system shutdown on a 2200T device using the SMS or the CLI causes the system to reboot instead of keeping the system powered down.	SEG-115592
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
SSL inspection cannot occur when web mode is enabled. By default, web mode is disabled.	TIP-64243
1G fiber module does not support auto-negotiation. SMS will currently report auto-negotiation as enabled; however, any changes from SMS, LSM, or CLI will not take effect.	TIP-66924
In rare occurrences, the TPS does not decrypt sites and the connection will be blocked. If this occurs for sites that must be accessed, navigate to **Profiles > Shared Settings > SSL > Client > Decryption Policies > Domains** on your SMS and specify those sites in the do-not-decrypt list.	TIP-45656 TIP-49103
Deploying a vTPS in Performance mode fails when using version 6.7 of the ESXi Hypervisor. **Workaround:** To successfully complete a deployment in Performance mode using ESXi 6.7, follow these steps: 1. Deploy the vTPS in Normal mode. 2. Shut down the vTPS virtual appliance. If the appliance is managed, you can also shut it down from the SMS client by right-clicking the device on the Devices page and selecting **Edit > Device Configuration**. 3. Configure the vTPS parameters to 6 vCPUs and 16 GB memory. 4. Reboot the vTPS virtual appliance. The SMS automatically recognizes the resource allocation and changes to Performance mode. 5. Examine the output of the `show version` command to confirm that the device is now running in Performance mode.	SEG-76770

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
System logs do not indicate when the state of a transceiver changes.	TIP-39167
The TPS presents an untrusted certificate warning for some websites because it cannot verify the certificate chain. Administrators of these websites might not be aware that their sites are not configured with a proper certificate chain, since most browsers have developed ways to automatically work around this issue. Consider the following options for accessing such a website: • Use mechanisms specific to your browser to bypass the `Untrusted certificate` warning (for example, add an exception or proceed to the site anyway) • Have your administrator manually download an intermediate certificate, upload it to your device, and add it the Trust Store on your SMS. • Consider providing feedback to the website to inform its administrators that their site employs a misconfigured certificate chain.	TIP-37062

Product support

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