Threat Protection System Release Notes

Version 5.4.1

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.
- Use SMS v5.4.1 and later to manage a TPS device with this release. SMS v5.4.1 upgrades are only supported from an SMS installed with SMS v5.3.0. Attempts to upgrade to 5.4.1 from an older release will result in an error message. If the error message is blank, check the SMS system log for the entire error message.

Release Contents

Description	Reference
The following error no longer occurs during DNS Reputation filtering: `Error TOSPORT NP: <thread> DNS Decoder: Parse of generated NXDOMAIN PDU failed; disposition is npDispositionEthTypeUnknown`	TIP-39422
A filter targeted to be disabled through adaptive filtering configuration (AFC) is no longer re-enabled after a Reputation distribution.	TIP-35279
Attempts to contact the peer device during TRHA no longer cause the system to freeze.	TIP-56762
Profiles with an SSL inspection policy no longer fail to distribute to TPS 2200T devices.	TIP-57436
This release repairs an SMB flow issue in which Trust actions were slow to complete on 8200TX and 8400TX devices.	TIP-56512
An issue with the heartbeat from **healthcheckd** to **tosportd** that would generate a `TosPort process hang` message in the TSR log has been resolved.	TIP-47425
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
TPS devices that used a certificate from the default CA package for the inbound SSL proxy would not be able to receive profile distributions. This release relaxes the restriction that required users to remove any previously imported CAs before importing another default package that had overlapping CAs.	TIP-56688 TIP-56761

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, use the following commands:
 	
To keep the default value:
`debug ini-cfg modify netpal.ini.handle [fastPath] so-netconfig ""`
 	
To change the interval value to a specified number of seconds:
`debug ini-cfg modify netpal.ini.handle [fastPath] so-netconfig tcp.fintimeout=<seconds>`
 	
To turn off the interval setting and revert to the previous behavior:
`debug ini-cfg modify netpal.ini.handle [fastPath] so-netconfig tcp.fintimeout=0`
 	
Reboot your device after making any of these changes.
 	
Note: Use debug commands only when you are instructed to do so by TippingPoint product support.
	TIP-56189

Users who previously encountered an `SSL Inspection reached Critical threshold` notice in the system log, and who could not effectively modify their topology or application to close the connections, can now configure an SSL proxy idle timeout feature. After upgrading to TOS v5.4.1 or later, you can activate the timeout, which is disabled by default, using a debug command that includes a time value that you specify (in milliseconds). For example, to close SSL-proxied connections that have not forwarded application data for 10 minutes (600000 milliseconds), and thereby freeing appliance resources, enter the following command: `debug ini-cfg modify netpal.ini.handle [SslInsp] npSslIdleTimeoutMs 600000 create` Configure a value of `0` to disable the timeout and return to the default behavior. Reboot your device after making any of these changes. **Note:** Use debug commands only when you are instructed to do so by TippingPoint product support.	TIP-56250
When you configure outbound client SSL inspection, the following settings no longer cause server traffic to the client proxy to drop: • Client proxy's decrypted service is set to 'other,' and • IPS deployment type is set to 'Performance-optimize' or 'Security optimized'	TIP-53731

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
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
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
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.	TIP-37062

• Consider providing feedback to the website to inform its administrators that their site employs a misconfigured certificate chain.	
System logs do not indicate when the state of a transceiver changes.	TIP-39167
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)*.