Threat Protection System Release Notes

Version 5.4.0

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 v5.3.1 before installing this version. Learn more.
- Use SMS v5.4.0 and later to manage a TPS device with this release. SMS v5.4.0 upgrades are only supported from an SMS installed with SMS v5.3.0. Attempts to upgrade to 5.4.0 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
With TOS v5.4.0, TPS devices provide in-line, real-time threat protection for both inbound server SSL traffic and outbound client SSL traffic.	New
TOS v5.4.0 includes support for the TLSv1.3 protocol and six new cipher suites, including TLSv1.3-specific ciphers. Learn more from the *SSL Inspection User Guide*.	New
The `debug congestion visibility` command has been added so you can view how uninspected traffic correlates to any systems or applications that might have been having issues during the congestion period. **Note:** Use debug commands only when you are instructed to do so by TippingPoint product support.	New
A new `ipsprefs` option has been added to the `display conf running` command that enables device configuration information (except policy settings) to be displayed.	New
In some circumstances, a system crash would prevent users from logging in and would prevent recovery mode. With this release, the console enters recovery mode within minutes of the crash, which enables a TSR, a system reboot, and service mode.	TIP-50225
The HTTP Response Processing default setting **Accelerated inspection of encoded HTTP responses** can now be changed to **Inspect encoded HTTP responses**.	TIP-49369
The remote syslog output now includes a **${deviceFQDN}** field that provides both the fully concatenated device hostname label and the fully qualified domain name. This enables some users to distinguish their devices according to the storage rack in which they are connected.	TIP-44717
The **cs5** Field for Arcsight CEF Format v4.2 no longer disappears from the remote syslog output.	TIP-45991
Rolling back to a parent profile after an upgrade no longer puts the device into a processing loop.	TIP-46507
Serializing a device object caused all devices and device groups in the tree to be serialized also. This caused devices sent to the client to congest the queue. This issue has been resolved.	TIP-44446
A memory leak no longer occurs when you enable the Filter Performance Correlation feature.	SEG-78618
Some customers noticed constant TCAM errors after upgrading their devices. This issue has been resolved.	TIP-47882
The `debug snmp trap` command has been added to enable you to test SNMP trap functionality for TPS devices. **Note:** Use debug commands only when you are instructed to do so by TippingPoint product support.	TIP-46338

The `chpasswd` command no longer fails to recognize the user name.	TIP-48275
SSL inspection over VxLAN is now supported.	TIP-45678 TIP-45595

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
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
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	SEG-76770

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.	
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
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
System logs do not indicate when the state of a transceiver changes.	TIP-39167

Any TPS devices running TOS v5.4.0 that use a certificate from the default CA package for the inbound SSL proxy will not be able to receive profile distributions. A message similar to the following identifies the condition in the SMS system log:
`Time      Severity Message`
`10/6/20 3:43:58 PM PDT     Error    ngfw.cert.device.bulk.create.err`
`10/6/20 3:43:58 PM PDT     Error    Distribution to device device failed: org.xml.sax.SAXParseException; lineNumber: 1; columnNumber: 1; Content is not allowed in prolog.`
`10/6/20 3:43:58 PM PDT     Error    Profile distribution to device device: Failed (Install failed: ngfw.cert.device.bulk.create.err (device)`
`10/6/20 3:43:58 PM PDT   Error   SMS: device (10.11.12.13) System Log Notification (error): SOAP Daemon: SOAP RC CHECKF (rc=-1): Certificate 'Outbound_Root' has already been imported with name: Entrust Root Certification Authority - G2(There are total 2 CRIT/ERR messages, please check device's system log for details.`
`10/6/20 3:43:58 PM PDT     Error    SMS: device  (10.207.8.218) System Log Notification (error): SOAP Daemon: SOAP RC CHECKF (rc=-1): Certificate 'Outbound_Root' has already been imported with name: Entrust Root Certification Authority - G2`
 	
If your device is in this state, contact Support (https://tmc.tippingpoint.com/TMC/Support?parentFolderId=support&contentId=Support_Contacts) for a workaround until the issue can be fixed in a maintenance release.
	SEG-88673

When you configure outbound client SSL inspection, the following settings could 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' To avoid this, disable filter 0559.	TIP-53731

Product support

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