Intrusion Prevention System Release Notes

Version 3.9.4

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

Important notes for IPS

- Before you upgrade your device to the latest TOS, maximize the space on your device by removing outdated TOS versions and packet traces that are no longer required. This ensures a successful upgrade and allows for a TOS rollback, if necessary. You can remove previous TOS versions using the SMS, the LSM, or the CLI.
- After installing this release, update the DV package to the latest version.
- Use SMS v5.0.1 Patch 1 or later to manage a device with this release.

Release Contents

Description	Reference
The `quarantine list` CLI command now accepts up to 60 characters to accommodate IPv6 addresses.	121692
When packet trace flags are reset, the device no longer removes data from events in the block/alert logs.	123734
Third-party authenticated vulnerability scans of the IPS management port no longer cause the device to enter into Layer 2 Fallback.	104236
An issue that caused a false positive no longer affects Filter 7170.	119668
Incrementing XGMII drops no longer cause a spike in network latency.	123319
A stacking heartbeat timeout no longer causes a stack to enter Layer 2 Fallback.	124401
Fragmented DCE/RPC traffic drops no longer cause devices to go into Performance Protection mode.	116304
The `debug np mcfilt-regex` command no longer includes invalid results.	125118
This release reduces the benign error `Get Policy Details failed to get SZP using np handle [1]` to a warning in the system log.	124919
After a reboot, the IPS generated a `Failed to allocate sortList storage` error when the device was not ready to accept stats polling. For better clarity, the `Regex stats are not available until runlevel 12 has been reached` error is now displayed in the system log when the device is in this state.	123220
Supported attributes for the tptHardwareNotifyHlStateQual MIB object have been documented in the *MIBs Guide*.	116727
Issues that caused filters to trigger on inapplicable traffic have been resolved.	121253, 118255
An issue no longer occurs that caused the IPS to crash during a reputation DV distribution.	122653
When the CPU was prevented from receiving a heartbeat message, the device would enter L2FB.	122753
Certain conditions no longer prevent Scan/Sweep filters from firing.	124905
Leftover reputation packages that caused UDM load fail errors are now properly removed.	124004, 124555

Devices no longer route all VLAN traffic to the same thread.	125860
You can now disable cipher suites using the CLI.	126049
The SMS no longer reorders virtual segments incorrectly after it manages a device with a new ANY-ANY segment created by the LSM or CLI.	116675
IPS inspection performance of RPC and SMB traffic has been improved.	125878
A best effort mode issue that could result in increased latency and reduced throughput without packet loss no longer occurs.	116536

Known issues

Description	Reference
Reference Devices configured to connect to an NTP server using the server hostname no longer connect to the NTP server after a reboot. To avoid this issue, always establish an NTP server connection using the IPv4/ IPv6 address of the NTP server.	118020
Microsoft Edge or Microsoft Internet Explorer might not connect to the LSM. To resolve this issue, use the `conf t server` TLS command to enable TLS v1.0 on the IPS security device. Be aware that TLS v1.0 is a weak encryption algorithm. Consider using another supported browser instead. For more information about using the `conf t server` command, refer to the *IPS Command Line Interface Reference*.	117878
A profile distribution issue can degrade system performance, including dropped packets and a spike in XLR utilization. A filter reset temporarily clears the condition.	124604
Modifying a profile or changing which profile is applied to the ANY-ANY virtual segment of a device, *while that device is unmanaged from SMS*, can cause an out-of-sync condition when the device is remanaged to the SMS. The recovery for the out-of-sync condition is to reboot the device. To avoid this condition, make changes to the ANY-ANY virtual segment only through the SMS.	124603
Common CIDRs, such as /56 and /64, cannot be used for IPv6 bypass rules.	124529

Product support

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