Intrusion Prevention System
Release Notes

Version 3.9.7

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- Before you upgrade your device to the latest TOS, maximize the space on your device by removing outdated TOS versions and packet traces that are no longer required.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 2 or later to manage a device with this release.

Release Contents

Description	Reference
Support for additional AES-CTR cipher suites for SSH device management is now available on N/NX systems. These new cipher suites are available on all FIPS modes (disabled, crypto, and full). **SSH ciphers** AES128-CTR, AES192-CTR, AES256-CTR **Key Exchange:** diffie-hellman-group-exchange-sha256 **MACs:** hmac-sha2-256, hmac-sha2-512	TIP-61678 SEG-71993 SEG-90695
Only AES-CTR SSH cipher suites are enabled when the device is in CRYPTO or FIPS FULL mode. If your device is configured for FIPS CRYPTO or FIPS FULL and you require older ciphers for compatibility, you must disable FIPS mode prior to upgrading to TOS 3.9.7.	

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-61165
Rapidly clicking the Test button during remote authentication server configuration no longer results in an LSM failure.	TIP-62335 SEG-84147
Attempting to start a traffic capture in quick succession with an invalid tcpdump expression syntax no longer results in a device failure.	TIP-62337 SEG-91073

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
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)*.