Firmware for TN-4900 Series Release Notes

Version: v3.13	Build: 24100800
Release Date: Oct 09, 2024	

Applicable Products

TN-4900 Series

Supported Operating Systems

N/A

New Features

• Added support for the Loopback Interface function.
• Added support for event-triggered actions to the VRRP function.
• Added support for UDP-Flood to the DoS Policy function.
• Added SNMP Trap as a Log Destination for the Layer 2 Policy function.
• Added support for additional event log export formats: .pdf, .csv.
• Added a CPU usage threshold alarm to the Event Notifications function.
• Added a port usage threshold alarm to the Event Notifications function.
• Added support for Step7 Comm+, OPC UA, and MELSEC to the Advanced Protection function.
• Added support for save and restore to the Custom Default function.
• Added support for the DNS Server function in Network Service.

Enhancements

• Enhanced the following IPsec algorithms:
Encryption: AES-256-GCM
Hash: SHA-512
DH Group: DH15 (modp3072), DH16 (modp4096), DH17 (modp6144), DH18 (modp8192), DH22 (modp1024s160), DH23 (modp2048s224), DH24 (modp2048s256), DH31 (curve25519)
PRF: PRF SHA-256, PRF SHA-384, PRF SHA-512
• Added a syslog option for VRRP State Change notifications.
• A detailed log message will now be recorded when importing a configuration fails.
• Supported Multiple Static Multicast Route Rules can be created with the same group address & outbound interface but different inbound interfaces.
• Added support for DHCP error logs in Event Notifications.
• Added support for IGMP Snooping error log in Event Notifications.
• Added support for the TRDP protocol to the Advanced Protection function in the CLI.
• Added support for RFC 5424 format for syslog messages.
• Added support for Default Action Log to the Layer3-L7 Policy function.

Bugs Fixed

• The "Login Authentication Failure Message" does not save properly.
• Using the newline character (\n) in the 'Login Message' and 'Login Authentication Failure Message' causes abnormalities in the output.
• The system is unable to ping the VRRP virtual IP.
• Users are able to bypass password policy violation warnings by pressing ESC on the keyboard.
• Time zone settings are not saved if GMT is set to 0.
• Port-based DHCP provides the same IP if those ports are member ports of a created bridge interface.
• RSTP is not functioning correctly over VLAN trunk ports.
• RSTP on VLAN trunk ports is causing a dual root device situation.
• Only one static multicast address can be configured at a time using the CLI or web import.

• SNMP OID returns an additional "\n" character.
• NAT is not working after reboot.
• op-up window will stay after auto logout.
• CVE-2024-6387 vulnerability issue. For more details, search the Security Advisories section on the Moxa website using the following Security Advisory ID: MPSA-246387.
• CVE-2024-9137, CVE-2024-9139 vulnerability issues. For more details, search the Security Advisories section on the Moxa website using the following Security Advisory ID: MPSA-241154.
• CVE-2024-1086 vulnerability issue. For more details, search the Security Advisories section on the Moxa website using the following Security Advisory ID: MPSA-249807.

Changes

• Changed the IPS license expiration behavior: When the license expires, IPS functionality will remain enabled, but IPS patterns will no longer be updated.
• Changed the Trusted Access behavior: Trusted Access now applies to the Web UI, CLI, and New Moxa Command interfaces.
• Changed the Preempt Delay range for the VRRP function from 10 to 300 to 0 to 300.
• Changed the maximum password and shared key length to 64 characters.
• The password and shared key now support special characters.

Notes

• If you encounter unexpected behavior with ECSP control packets, try disabling the Trusted Access Function first. If the issue persists, please contact the MOXA Technical Support team.