Illumio® NEN

Version 2.5.2
PCE Versions: 21.5.1 - 22.5.x

Release Notes

12/06/2022
29000-100-2.5.2

Contents

About this Document

These release notes describe the new features, enhancements, resolved issues, and known issues for the Network Enforcement Node (NEN) 2.5.2 release.

The NEN is the Illumio Core switch and Server Load Balancer (SLB) interface that provides visibility and enforcement on switches and SLBs.

See the *NEN Installation and Usage Guide* for information.

Document Last Revised: December 2022
Document ID: 29000-100-2.5.2

What's New In This Release

To learn what's new and changed in 2.5.2, see *What's New in This Release* in the *Illumio NEN Installation and Usage Guide*.

Product Version

NEN Version: 2.5.2
Compatible PCE Versions: 21.5.1 – 22.5.x

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see **Versions and Compatibility** in the Illumio Support portal (log in required).

Release Types and Numbering

Illumio Core release numbering uses the following format: "a.b.c-d+e"

- "a.b": Standard or LTS release number, for example "2.2"
- ".c": Maintenance release number, for example ".1"
- "-d": Optional descriptor for pre-release versions, for example "preview2"

Resolved Issues in NEN 2.5.2

- **Tamper checking was prevented on the SLB** (E-98697)
  In some circumstances, the PCE may inform the NEN that there is a policy update for an SLB when there isn't actually an update. This may prevent the NEN from running tamper checking on the SLB. To help resolve this condition going forward, if the NEN is told about a non-existent policy update for the SLB and the time for performing a tamper check has lapsed, the NEN will now perform a full policy check for the SLB.
- **Problems caused when deleting a VS before unmanaging it on the PCE** (E-97909)
  Deleting an enforced VS from an SLB without first unmanaging the VS on the PCE interfered with the NEN's attempt to remove policy from the SLB, which prevented the NEN from correctly handling error responses from the SLB. This caused the NEN to:
    - Retry removing policy multiple times, which put a load on the SLB.
    - Run multiple simultaneous SLB programming jobs.
  This issue is resolved. Now, the NEN no longer retries sending APIs requests when 4xx API response codes are returned during the removal of policy from a VS and only runs one programming job per SLB at a time.

Known Issues in NEN 2.5.2

There are no known issues in this release.

Resolved Issue in NEN 2.5.1

Excessive NEN API GET calls to F5 prevented policy programming (E-96989)

When trying to unmanage F5 Virtual Servers, NEN API GET requests to the F5 encountered slower than expected response times, which lead to the following sequence of events:

1. Responses from the F5 timed out.
2. Which in turn caused the NEN to retry its requests repeatedly.
3. Lacking timely F5 responses, the NEN ran multiple simultaneous unmanage jobs for VSs.
4. This caused the NEN to DDOS the F5 with `GET /mgmt/tm/security/firewall/policy?expandSubcollections=true` API calls.
5. **Result:** This overloaded the F5 and caused policy programming to fail due to API timeouts.

This issue is resolved. The NEN now serializes unmanage VS jobs for server load balancers.

Known Issues in NEN 2.5.1

There are no known issues in this release.

Resolved Issues in NEN 2.5.0

- **When processing multi-paged AVI API responses, policy programming failed** (E-95740)
  While processing multiple-paged AVI `networksecuritypolicy` API responses during policy programming, the NEN incorrectly stored the policy ID to associate the policy to its rules. This caused the NEN to point to an invalid memory location, which in turn caused `network_enforcement_policymgr` to crash and policy programming to fail. This issue is resolved.

- **Problem when tamper checking AVI SLBs in multi-page AVI API responses** (E-95546)
  An invalid check of the returned API response occured when the NEN performed tamper checking of multiple-paged AVI `networksecuritypolicy` API responses. This issue could have caused the NEN to miss some Illumio `networksecuritypolicies`. The NEN could then have interpreted the missed policy as policy tampering, triggering a check on the SLB for those missing policies, resulting in no errors found. The issue was resolved by fixing the API response checks to make sure the NEN retrieved all `networksecuritypolicies` from the AVI SLB.

- **Generating switch policy failed in an HA configuration** (E-94344)
  Generating policy by running the switch policy generate command on the primary node of an High Availability (HA)-configured NEN (from either the UI or from the CLI) could cause policy generation to fail and return the following error message: *This command can only be run on the node running the primary Network Enforcement Service*. This issue is resolved. The command can now be run on any NEN node – primary or secondary – that is running the `network_enforcement` service.

- **Policy update failed when new Illumio iRules weren't applied correctly** (E-93921)
  An error occurred when trying to create a policy that applied a new Illumio iRule to block an existing non-Illumio iRule. The error prevented policy from being updated. This issue is resolved. New Illumio iRules are now applied before non-Illumio iRules.

- **PCE sent multiple unnecessary policy updates to the NEN** (E-93851)
  Illumio updated the NEN 2.5.0 to address this issue in the PCE. In previous releases, the PCE sent policy updates to the NEN even when the SLB virtual services address list hadn't changed. This issue occurred because pods frequently go down and come back up and that

triggered a policy job with "no address list changes" in the PCE. In this release, this issue is resolved for the NEN. The issue will be resolved in the PCE in a future release. In this release, the NEN optimizes the addresses in the address list and stores the SHA of the sorted address list for comparison between policies. The PCE ignores policy updates that don't contain changes in the overall address list by comparing the SHA of new address list with the previous one.

- **F5 AFM policy deletion for a deleted VS failed** (E-92008)
  When a NEN tried to delete a policy from an F5 BIG-IP Advanced Firewall Manager (F5 AFM) for a virtual server (VS) that had been deleted, the NEN defaulted to treating the VS like a non-AS3 managed VS. This resulted in the policy remaining on the F5 AFM. This issue is resolved and the NEN now makes sure (as originally intended) that no artifact of a policy remains on the SLB for the deleted VS.

Known Issues in NEN 2.5.0

There are no known issues in this release.