SP 800-90B Non-Proprietary Public Use Document
Junos OS™ Entropy Source version 22.4
Document version 1.1
Firmware version 22.4

Juniper Networks, Inc.
1133 Innovations Way
Sunnyvale, CA 94089
United States

Revision History

Version	Change
2023-09-27	Initial draft
2023-10-18	Removed unnecessary reference to H_submitter.

Table of Contents

Description

This Junos OS™ Entropy Source is a non-physical (NP), non-IID source specific to version 22.4 of the firmware and is bound to the following module on which it was tested:

- EX4100 (ARM-cortex A72 64-bit, single core)

The security boundary of the entropy source coincides with the FIPS 140-3 cryptographic boundary of the modules listed above, which are multiple-chip standalone modules running a limited operational environment.

Security Boundary

The security boundary of the entropy source coincides with the cryptographic boundary of the modules listed above, which is the outer edge of the chassis. These cryptographic modules consist of production grade components enclosed in a production grade removable metal enclosure.

Operating Conditions

The Junos OS Entropy Source operates correctly within the same range of operating conditions that apply to the modules on which it was tested. Normal operation is ensured under the following conditions:

- Temperature: 0-40 degrees Celsius
- Altitude: up to 10,000 ft
- Humidity: 5-90%, non-condensing

The entropy source does not require the module to be placed in FIPS mode.

Configuration Settings

The entropy source does not require any configuration.

Physical Security Mechanisms

The entropy source requires the same physical security mechanisms required by the cryptographic modules on which it was tested. These are described in the FIPS Security Policies of those modules.

Conceptual Interfaces

The GetEntropy interface is called by the Junos OS kernel DRBG for seeding and reseeding purposes.

Min-Entropy Rate

The Junos OS Entropy Source provides 448 bits of min-entropy per 512 bit output sample.

Health Tests

The entropy source implements the following health tests:

- Repetitive Count Test conforming to NIST SP 800-90B section 4.4.1:

    - *H* = 1 bit of entropy per 8-bit sample;
    - Cutoff value *C* = 21.
- Adaptive Proportion Test conforming to NIST SP 800-90B section 4.4.2:
    - *W* = 512;
    - *H* = 1 per 8-bit sample;
    - Cutoff value *C* = 311.

In conformance with NIST SP 800-90B, these health tests are performed in three circumstances:

- Start-up Tests: The entropy source performs start-up APT and RCT health tests on 1024 samples. If either of these tests fail, the count of samples is reset to zero and the start-up tests are performed again. The entropy source does not output any data until both the requisite number of samples has been collected and the start-up health tests have passed.
- Continuous Tests: The entropy source performs continuous APT and RCT tests during operation. If either of the tests fail, the sample count is reset to zero and the start-up health tests are performed again. The entropy source will not output data until the health tests have passed.
- On-Demand Tests: The entropy source will perform on-demand tests when the cryptographic module is restarted.

Maintenance

This module does not require any maintenance

Required Testing

The module performs both start-up and continuous health tests as per NIST SP 800-90B. The start-up health tests may be triggered by rebooting the device.

The Junos OS Entropy Source was tested in accordance with NIST SP 800-90B requirements. Both and raw and restart data were collected by the vendor. No further testing is required.