

# SP 800-90B Non-Proprietary Public Use Document

## Entropy Source: Switch Engine Entropy Source
## Version: 33.4.1

Document Version: v1.1.2
Date: May 1, 2026


Prepared By:

**KeyPair Consulting Inc.**
987 Osos Street
San Luis Obispo, CA 93401
United States

Prepared For:

**Extreme Networks, Inc.**
2121 RDU Center Drive
Morrisville, NC 27560
United States

# References

| Ref | Title | Date | Author |
|---|---|---|---|
| [SP 800-90B] | NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation | 10-Jan-2018 | NIST CT |
| [140IG] | Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program | 27-Feb-2026 | NIST CMVP |
| [140MM] | FIPS 140-3 CMVP Management Manual, §4.8 Entropy Source Validation (ESV) Processes | 16-Oct-2025 | NIST CMVP |
| [JEnt] | Jitter Entropy Library v3.4.0 | 04-Feb-2024 | S. Müller |
| [LRNG] | Linux /dev/random – A New Approach | 28-Sept-2024 | S. Müller |
| [Müller 2022] | CPU Time Jitter Based Non-Physical True Random Number Generator | 01-Jul-2022 | S. Müller |
| [Heuristic] | Jitter Entropy Library v3.4.0-v3.6.1 Entropy Source Opportunistically Essentially-IID Heuristic Assessment Procedure | 20-Feb-2025 | J. Hill |
| [NIST Ent] | EntropyAssessment Tool. Version 1.1.8. | 12-Jul-2024 | NIST CMVP |
| [Theseus] | Theseus. Version 20250626. | 26-Jun-2025 | J. Hill |

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.

# Table of Contents

References ..... 2
1 Description ..... 4
2 Security Boundary ..... 6
3 Operating Conditions ..... 6
4 Configuration Settings ..... 6
5 Physical Security Mechanisms ..... 7
6 Conceptual Interfaces ..... 7
7 Min-Entropy Rate ..... 7
8 Health Tests ..... 8
9 Maintenance ..... 8
10 User Verification ..... 8

# List of Tables

Table 1. Evaluated Entropy Source Specification ..... 5
Table 2. Operating Environments ..... 6
Table 3. Entropy-Relevant Parameters (OE-specific) ..... 7

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.

# 1 Description

This Public Use Document accompanies the Extreme Networks, Inc. entropy source validation of the Switch Engine Entropy Source v33.4.1, which is included in Extreme Networks Switch Engine releases with versions of the form 33.4.1.x and 33.4.100.x. This entropy source is based on a modified version of the open-source Jitter Entropy Library Entropy Source v3.4.0 ("JEnt") included within a Linux v5.10.177 kernel using the LRNG v57 patch.

The entropy source is a non-physical entropy source intended to generate entropy input for instantiation and reseed of an SP 800-90A compliant DRBG. This entropy source has been evaluated for compliance to [SP 800-90B] and the [140IG], specifically FIPS 140-3 IG D.J (last modified on November 5, 2021) and IG D.K (last modified on March 17, 2023).

The entropy source design includes elements that map to the conceptual components contained within an SP 800-90B entropy source:

- The primary noise source (memory and conditioning timing).
- Health tests.
- A conditioning chain consisting of:
    - The JEnt SHA3-256 conditioning component.
    - The LRNG SHA2-256 conditioning component, which is vetted.

The output from each conditioning step is full entropy.

The only source credited as contributing entropy in this system is JEnt. All other sources are enabled and are considered additional noise sources within this design.

The JEnt design is depicted in Figure 1, with design documented in [Müller 2022, §3].

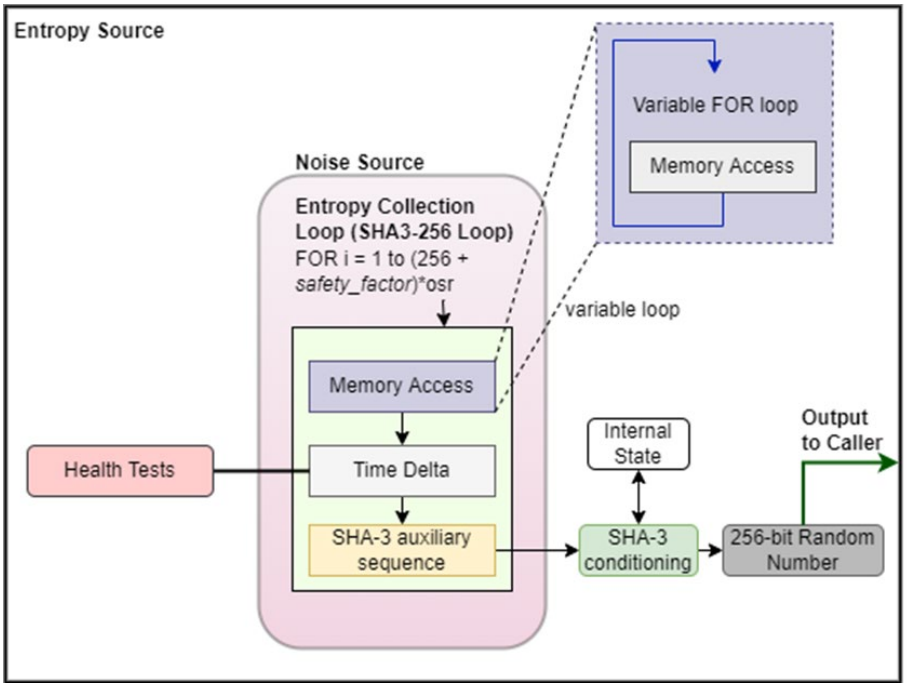



*Figure 1. Entropy Source Design (from [Heuristic])*

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.

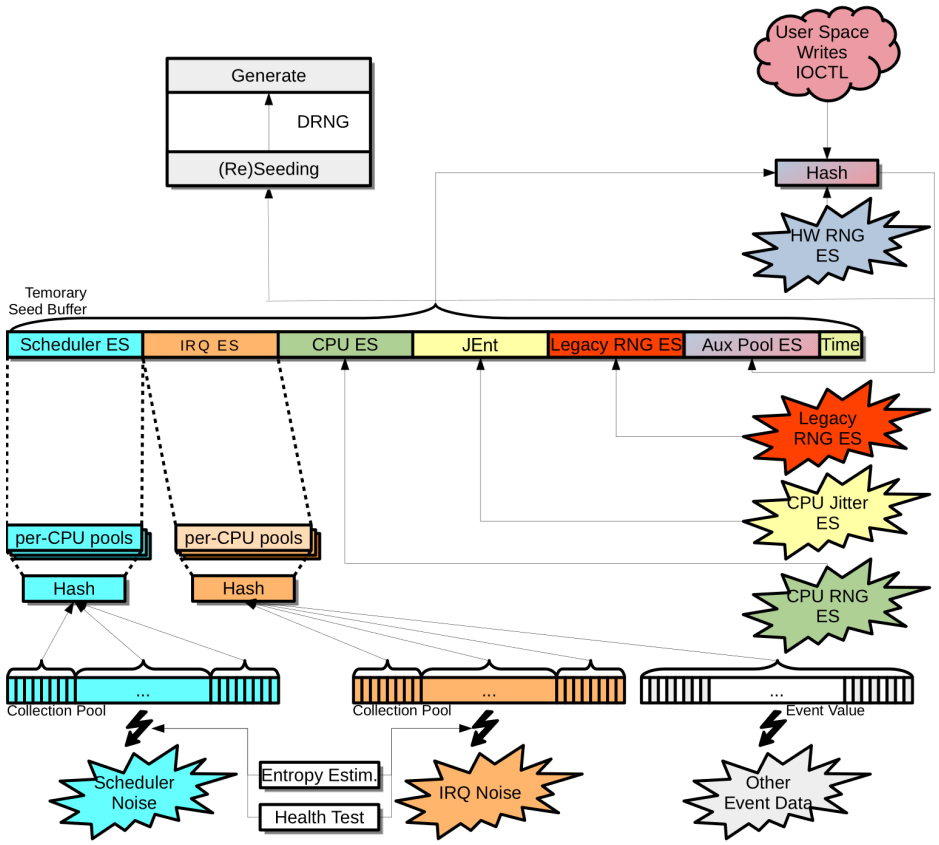



*Figure 2. LRNG Component of the Entropy Source Design (From [LRNG])*

This Public Use Document is constructed to support validation of multiple platforms within a general architecture. While the performance of JEnt is highly variable across variations in CPU and memory configuration, the selected sub-distribution entropy analysis approach permits a consistent Entropy Analysis Report and associated validation listing. The design of JEnt permits compile time configuration (here required to be consistent with the Operating Conditions and Configuration settings described below) that results in the entropy source providing full-entropy conditioned output.

*Table 1. Evaluated Entropy Source Specification*

| Identifier | Details |
|---|---|
| Entropy Source Name | Switch Engine Entropy Source |
| Software Version | 33.4.1 |
| Entropy Category | Non-physical (NP) |
| Entropy Estimation Track (per SP 800-90B §3.1.2) | Non-IID |

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.

*Table 2. Operating Environments*

| Operating Environment | CPU | Temperature | Humidity |
|---|---|---|---|
| 4120-24MW-4Y | Renesas RZ/G2E (ARM Cortex-A53) | 0-50C | 10-95% non-condensing |
| 4220-12T-4X | Broadcom BCM53642 (ARM Cortex-A72) | 0-50C | 10-95% non-condensing |
| 5320-24T-8XE | Broadcom BCM56175 (ARM Cortex-A72) | 0-50C | 5-95% non-condensing |
| 5320-48T-8XE | Broadcom BCM56274 (ARM Cortex-A72) | 0-50C | 5-95% non-condensing |
| 5420F-48T-4XE | Broadcom BCM56274 (ARM Cortex-A72) | 0-50C | 10-95% non-condensing |
| 5420M-16MW-32P-4YE | Broadcom BCM56275 (ARM Cortex-A72) | 0-50C | 5-95% non-condensing |
| 5520-12MW-36W | Broadcom BCM56375 (ARM Cortex-A72) | 0-45C | 5-95% non-condensing |
| 5720-48MW | Intel® Atom™ CPU C3338 (Denverton) | 0-50C | 5-95% non-condensing |
| 5720-48MXW | Intel® Atom™ CPU C3538 (Denverton) | 0-50C | 5-95% non-condensing |
| 7520-48Y-8C | Intel® Atom™ CPU C3758 (Denverton) | 0-50C | 10-95% non-condensing |
| 7720-32C | Intel® Atom™ CPU C3758 (Denverton) | 0-50C | 10-95% non-condensing |

**The entropy assessment findings and the validation described by this Public Use Document are specific to the particular parts/versions and entropy-relevant parameters given in this document and do not apply more broadly. If the entropy-relevant parameters are different than those described in this document, then additional modeling and statistical testing are required. Any part/version or configuration other than that described herein is not covered by this validation.**

# 2 Security Boundary

The entropy source boundary includes the identified JEnt library and the hardware necessary to run it within the computational environment, consistent with [Heuristic §1.2]. See Figure 1 and Figure 2 for block diagrams depicting this entropy source.

# 3 Operating Conditions

The operating environments specified in Table 2 are expected to behave consistently across the full range of the environmental conditions supported by their underlying hardware.

# 4 Configuration Settings

The entropy source is compliant to the requirements of SP 800-90B when one of the referenced versions of the firmware is running on the listed hardware; there is no additional configuration that is required.

These details can be verified by using the *show version* command on the command line interface (CLI), which describes the image in use as "`Extreme Networks Switch Engine version <version specification>`". This version specification must be one of the Switch Engine 33.4.1 family (e.g., "33.4.1.x" and "33.4.100.x"), all of which include this entropy source.

Entropy relevant parameters are listed in Table 3 (parameters specific to a platform and an associated operating and analysis configuration); these parameters are set by the firmware in use and are not adjustable by the user.

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.

*Table 3. Entropy-Relevant Parameters (OE-specific)*

| Operating Environment Class | Operating Environment | JENT_MIN_OSR[1] Lower Bound |
|---|---|---|
| ARM | 4120-24MW-4Y | 19 |
| | 4220-12T-4X | |
| | 5320-24T-8XE | |
| | 5320-48T-8XE | |
| | 5420F-48T-4XE | |
| | 5420M-16MW-32P-4YE | |
| | 5520-12MW-36W | |
| X86 | 5720-48MW | 84 |
| | 5720-48MXW | |
| | 7520-48Y-8C | |
| | 7720-32C | |

# 5 Physical Security Mechanisms

The Switch Engine Entropy Source operates within the physical protections of the associated processor.

The JEnt design may be incorporated into modules intended for CMVP validation of compliance to FIPS 140-3 and the related suite of security assurance standards and specifications. Any additional physical security protections are outside the scope of this entropy source design and implementation.

# 6 Conceptual Interfaces

The entropy source is depicted in Figure 1.

Data output from the validated LRNG DRBG is available using the /dev/random device or the `getrandom` call (when not using the `GRND_INSECURE` flag).

When reading data from /dev/random that was opened with `O_SYNC` or using `getrandom` with `GRND_RANDOM`, a special DRBG (DRNG) instance that operates with prediction-resistance is used; in this instance generate calls are limited to 256 bits per generate.

# 7 Min-Entropy Rate

The Entropy Analysis Report concludes that the conditioned output of this entropy source is full-entropy; that is, the analysis supports the claim of 256 bits of min entropy per 256-bit conditioned output block, provided the platform-specific conditions and configuration settings described above are met.

These blocks are the output of a vetted conditioning function and can be subdivided further (as per SP 800-90B). If these blocks are subdivided, then every byte from the block can be treated as possessing at least 8 bits of min entropy, and the min entropy of any truncated sub-portion of the 256-bit output block is linearly scaled with the length of the retained sub-portion.

The output of this entropy source is used to seed the validated LRNG DRBG, using two blocks (512 bits) of full-entropy data to both Instantiate and Reseed the LRNG DRBG.

The LRNG DRBG is validated to comply with the requirements of SP 800-90A (AES-256 CTR_DRBG, CAVP certificate A7349).

[1] This macro was backported from the mainline JEnt library.

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.

# 8 Health Tests

On initialization the entropy source runs its start-up health tests. Once the entropy source is instantiated, all health tests are essentially continuous health tests and are tested within the `jent_read_entropy` function. This entropy source uses a modified version of the Repetition Count Test (RCT) and an Adaptative Proportion Test (APT).

When the health tests fail, the `health_failure` value is set to indicate the style of failure, signaling that the entropy source has encountered a fatal error. At this point all calls to `jent_read_entropy` will indicate a persistent health failure.

In normal use, this JEnt source is only used to instantiate and reseed the DRBG underlying /dev/random and the `getrandom` function call. When used as described above, these interfaces will block in the instance where instantiation or reseeding has failed.

The targeted cutoff parameters for the APT and RCT are set on compilation. Only raw data that passes all health tests is sent into the conditioner.

All of the start-up tests (the full set of continuous health tests) take the first 1024 consecutive samples. Some of the architectural health tests are run on the first 1124 samples.

On-demand testing is performed by rebooting. All samples tested by the start-up/on-demand health tests are discarded.

There is no mechanism to clear an error state short of rebooting or re-creating a new instance of the entropy source.

# 9 Maintenance

The Switch Engine Entropy Source does not require maintenance.

# 10 User Verification

The user of the system can output the contents of /proc/lrng_type. An example of the relevant portions of the output from this file is as follows:

```
DRNG name: drbg_nopr_ctr_aes256
LRNG security strength in bits: 256
…
Standards compliance: SP800-90C, NTG.1 (2011)
LRNG minimally seeded: true
LRNG fully seeded: true
LRNG entropy level: 256
…
Entropy Source 2 properties:
 Name: JitterRNG
 Available entropy: 256
 Enabled: true
 Jitter RNG async collection true
```

This output indicates that the JEnt library health tests have passed and are being used to seed the validated LRNG DRBG.

Copyright © 2026 Extreme Networks, Inc.

This non-proprietary document may be freely reproduced and distributed in its entirety without modification.