napa:tech;
SMARTNIC+DPU SOLUTIONS

Link-Capture™ Software

Suricata

SOLUTION DESCRIPTION

Increasing Suricata Performance

Link-Capture™ Software for Napatech SmartNICs

For Intrusion Detection and Prevention (IDS/IPS) implementations, missing any significant fraction of network traffic is unacceptable, as even a single packet not inspected by the IDS/IPS represents a blind spot for the security team.

Suricata detects known threats, policy violations and malicious behavior. However, as capable as Suricata is in reactively protecting a network, it will only be as effective as its implementation. Examining the contents of every network packet is extremely CPU-intensive, especially for a multi-gigabit traffic load. And this is often the limiting factor in Suricata performance: the packet processing on the CPU.

The Napatech Difference

In addressing this challenge, Napatech has created a hardware acceleration solution that alleviates the load on the CPU and thereby greatly increases Suricata performance. The solution is based on the Napatech Link-Capture™ Software, which is uniquely suited for lossless acceleration of Suricata. It offloads processing and analysis of networking traffic from the application software, while ensuring optimal use of the standard server's resources leading to effective application acceleration.

Optimized to capture all network traffic at full line rate, with almost no CPU load on the host server (all frame sizes), the solution demonstrates substantial lossless performance advantages for Suricata compared to a standard Network Interface Card (NIC):

- Dramatically increased lossless packet performance
- 100% lossless capture of all network traffic
- 50% higher maximum throughput
- Stateful flow awareness to block traffic in hardware

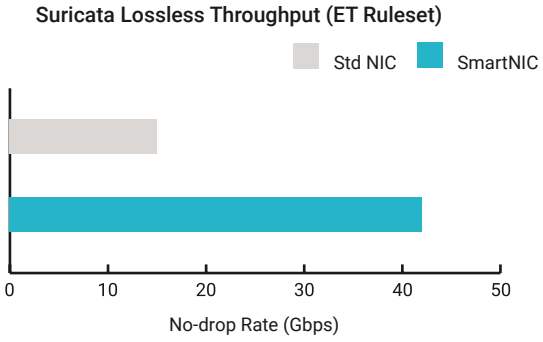
Turning Acceleration into Value

These performance advantages allow users to:

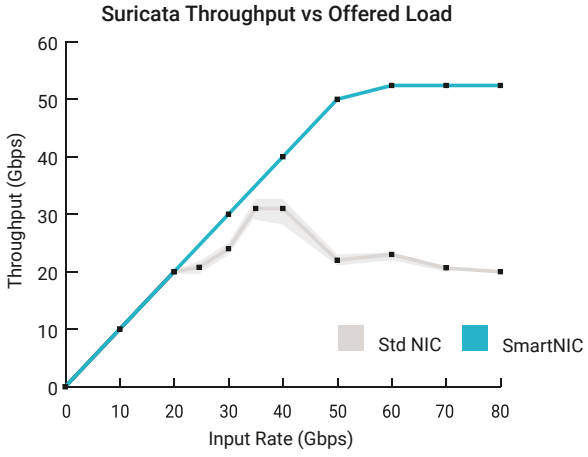
- Maximize server performance by improving CPU utilization
- Minimize TCO by reducing number of servers, thus optimizing rack space, power, cooling and operational expenses
- Diminish time-to-resolution, thereby enabling greatly increased efficiency

Outstanding Lossless Performance

The improvements achieved with this solution were demonstrated by comparing Suricata performance running on a Dell PowerEdge R740 with a standard 40G NIC card and the Napatech SmartNIC.



Using 40 cores (80 worker threads) on both sockets, the Napatech SmartNIC with Link-Capture™ Software provides much greater lossless Suricata packet throughput compared with a standard NIC when running Suricata with a 12,712-signature Emerging Threats ruleset.



Maximum Throughput

Running Suricata on all 40 cores, system throughput peaked at 34.8 Gbps with a standard NIC, while the Napatech SmartNIC delivered 50% higher maximum throughput.

Stateful Flow Awareness

By adding stateful flow awareness via a Napatech SmartNIC, CPU-intensive applications like Suricata are able to analyze network traffic on a per-flow basis for millions of flows to determine the required hardware-based processing. Programmatically, via standard APIs between Suricata and the flow-based SmartNIC, actions for individual flows can be updated in real time to be filtered or forwarded in hardware. This solution gives control back to the user providing additional computation to the application by reducing the amount of data needed for processing as certain flows or protocols no longer need monitoring and can be forwarded from port-to-port or blocked in hardware.

Deterministic Performance

Using the Napatech SmartNIC, Suricata demonstrates deterministic performance across all packet sizes. In contrast, standard NICs display significant variations in performance across a set of measurements with an identical workload. This behavior is shown in the graph above, where the Suricata performance utilizing the Napatech SmartNIC appears as a single sharp line indicating no variability. For the standard NIC, the thick grey line represents the average throughput value and the surrounding shaded band indicates the variation from various trials. In simple terms, the SmartNIC offered guaranteed application performance while the standard NIC performance varied by as much as 50% in test runs with the same offered load.

Test Configuration

The test configuration was based on a dual-socket Dell R740 with Intel® Xeon® Gold 6138 2.0 GHz, 128GB RAM running CentOS 7.5. Traffic was generated by PCAP replay of an actual network traffic capture comprising more than 125K flows with an average packet size of 486 bytes.

Key Solution Features

- Line rate network throughput for all packet sizes
- Lossless capture for perfect inspection and detection
- Onboard packet buffering during micro-burst or PCI Express bus congestion scenarios
- Advanced host memory buffer management for ultra-high CPU cache performance
- Packet classification, match/action filtering and zero-copy forwarding
- Intelligent and flexible load distribution to as many as 64 queues improving CPU cache performance by always delivering the same flows to the same cores

Napatech Link-Capture™ Software

The stunning benchmarks for Suricata were powered by Napatech's Programmable Computing Platform™, based on FPGA-based Link-Capture™ Software and Napatech SmartNIC hardware.

Napatech's Programmable Computing Platform flexibly offloads, accelerates and secures open, standard, high-volume and low-cost server platforms allowing them to meet the performance requirements for networking, communications and cybersecurity applications.

Suricata

Suricata is an ideal example of the type of critical enterprise security application that can achieve better performance through hardware acceleration. Suricata is a free and open source network threat detection application capable of real time IDS, IPS and network security monitoring. Suricata is architected with features specifically designed for performance and scalability:

- Multi-threaded code allows a single Suricata instance to utilize multiple CPUs
- Native support for specialized capture cards and hardware acceleration devices

Disclaimer: This document is intended for informational purposes only. Any information herein is believed to be reliable. However, Napatech assumes no responsibility for the accuracy of the information. Napatech reserves the right to change the document and the products described without notice. Napatech and the authors disclaim any and all liabilities. Napatech is a trademark used under license by Napatech A/S. All other logos, trademarks and service marks are the property of the respective third parties. Copyright © Napatech A/S 2025. All rights reserved.

DN-1187 Rev.4