napa:tech;
RECONFIGURABLE COMPUTING

Link™ Capture Software

Suricata

SOLUTION DESCRIPTION

4x Suricata Performance Increase

Link™ Capture Software for Intel® Programmable Acceleration Card with Intel Arria® 10 GX FPGA

For Intrusion Detection implementations, missing any significant fraction of network traffic is unacceptable, as even a single packet not inspected by the IDS 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.

In addressing this challenge, Napatech has created a hardware acceleration solution that alleviates the load on the CPU and thereby greatly increases Suricata performance. This has been achieved by making the Napatech Link™ Capture Software available for the Intel® Programmable Acceleration Card (PAC) with Intel Arria® 10 GX FPGA.

The Intel + Napatech Difference

The Intel PAC and Napatech Link™ Capture Software solution 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):

- 4 times lossless packet decode performance
- 100% lossless capture of all network traffic
- 40% improvement in CPU utilization

Turning Acceleration into Value

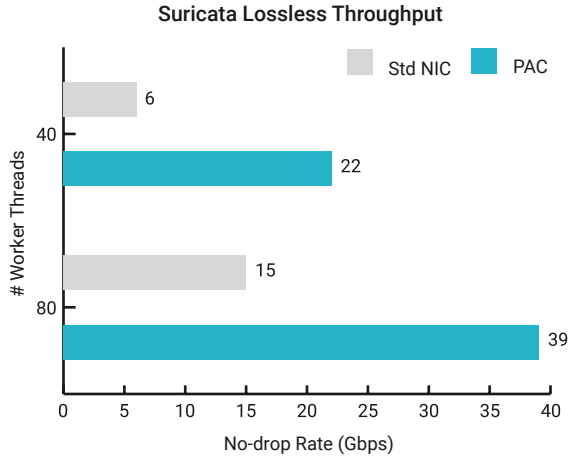
These performance advantages ultimately allow you to:

- Maximize your server performance by improving CPU utilization
- Minimize your TCO by reducing number of servers, thus optimizing rack space, power, cooling and operational expenses
- Diminish your 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 Intel PAC.

Using all 20 cores (40 HT) on a single socket, the Intel PAC with Napatech Link™ Capture Software provided much greater lossless Suricata packet throughput compared to a standard NIC when running Suricata with a 12,712 signature Emerging Threats ruleset. Using 40 cores (80 HT) on both sockets, the Intel PAC delivered 39 Gbps of lossless Suricata packet throughput, while the standard NIC peaked at 15 Gbps.



Maximum Throughput

Running Suricata on all 40 cores, the system topped out at 28.8 Gbps with a standard NIC, whereas the Intel PAC delivered 40 Gbps - demonstrating a 40% improvement in CPU utilization. The solution delivered a full 40 Gbps data stream to Suricata without loss while the host buffer utilization was barely measurable.

Test Configuration

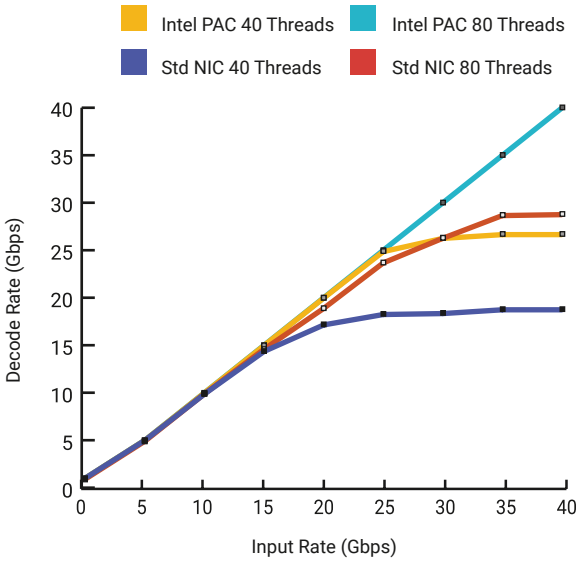
The test configuration was based on a dual-socket Dell R740 with Intel® Xeon® Gold 6138 2.0 GHz, 128GB RAM running CentOS 7.5. Traffic was generated by PCAP replay of an actual network traffic capture comprising more than 125K flows with an average packet size of 486 bytes.

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

Suricata Throughput

Decode Rate vs Offered Load (Emerging Threats Ruleset)



Napatech Link™ Capture Software for Intel® PAC

The Intel® Programmable Acceleration Card (PAC) with Intel Arria® 10 GX FPGA is a PCIe-based FPGA accelerator card for data centers supporting both inline and lookaside acceleration.

As the leader in FPGA-based SmartNIC software and hardware, Napatech has made its Link™ Capture Software available as an Acceleration Stack for the Intel PAC.

Napatech's Reconfigurable 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

Napatech helps companies to reimagine their business by bringing hyperscale computing benefits to IT organizations of every size. We enhance open and standard virtualized servers to boost innovation and release valuable computing resources that improve services and increase revenue. Our Reconfigurable Computing Platform™ is based on a broad set of FPGA software for leading IT compute, network and security applications that are supported on a wide array of FPGA hardware designs.