

Leveraging DYNANIC for Hardware Acceleration of Suricata Intrusion Detection System

Whitepaper prepared in collaboration with CESNET

Executive Summary

As network traffic grows in volume and complexity, Intrusion Detection Systems (IDS) like Suricata face increasing challenges in processing and analyzing data efficiently. Traditional software-only solutions often fall short in high-speed network environments, leading to packet drops and potential security blind spots. Hardware acceleration, particularly through the use of Field-Programmable Gate Arrays (FPGAs) and specialized network interface cards (NICs), offers a promising solution to this challenge. DYNANIC integrates these hardware acceleration techniques to significantly enhance the performance of Suricata IDS, reducing the need for extensive CPU resources.

This white paper outlines how DYNANIC supports hardware acceleration in IDS, the impact on CPU core usage, and the performance benefits realized through different levels of acceleration. The collaboration with CESNET has demonstrated that DYNANIC can effectively reduce the number of CPU cores required, allowing organizations to achieve better security performance with fewer resources.

Introduction

The increasing volume of network traffic presents a major challenge for IDS solutions like Suricata. Traditional software-based approaches struggle to maintain performance at modern network speeds, such as 100 Gbps and beyond. When traffic surpasses processing capacity, IDS systems may drop packets, creating potential security blind spots.

DYNANIC addresses these challenges as an FPGA-powered acceleration layer within the network interface card (NIC). This specialized firmware processes network traffic at the hardware level, streamlining data handling before it reaches the CPU. By optimizing traffic flow and offloading key processing tasks, DYNANIC enhances Suricata's performance, enabling more efficient threat detection while significantly reducing CPU dependency.

Hardware Acceleration in DYNANIC

DYNANIC's architecture offloads and optimizes network traffic processing directly within FPGA-powered NICs. This offloading is particularly effective in handling tasks such as Transport Layer Security (TLS) traffic prefiltering or traffic pattern matching. DYNANIC bypasses encrypted traffic that cannot be analyzed by IDS without decryption keys. TLS-prefiltered traffic is processed by the built-in deep packet scanning engine, which enriches packets with metadata about the detected patterns.

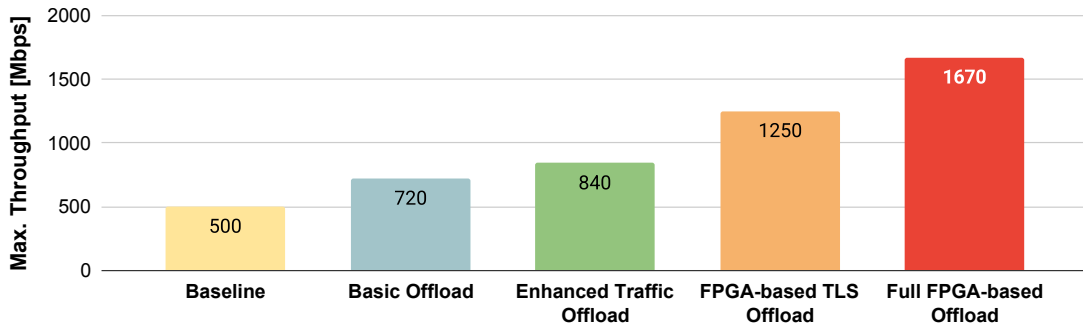
Key Features of DYNANIC Hardware Acceleration

- **FPGA-based Acceleration:** DYNANIC intelligently processes network data at the NIC level, offloading key operations such as encryption prefiltering and pattern-matching and reducing the load on Suricata’s CPU.
- **SmartNIC Integration:** SmartNICs equipped with FPGAs or other accelerators can handle complex tasks such as packet classification, which further reduces the CPU load.
- **Flexible Architecture:** DYNANIC’s modular design allows for easy integration with existing Suricata deployments, offering a scalable solution that can adapt to varying network conditions.

CPU Core Savings with DYNANIC

The use of DYNANIC can significantly reduce the number of CPU cores required to process network traffic in a Suricata-based IDS. The extent of CPU core savings depends on the level of acceleration implemented.

Impact of Different Levels of Hardware Acceleration



Suricata throughput per single CPU core for various types of hardware acceleration

- **Basic Traffic Offload:**
 - This mode uses fundamental traffic bypass techniques such as flow shunting and basic encrypted traffic bypass. In this configuration, Suricata remains in control, determining which flows should be bypassed and instructing the FPGA’s connection tracking table accordingly. The FPGA card filters out unwanted traffic.
 - **CPU Core Savings:** Up to 30% reduction in CPU core usage in a typical network environment.

- **Enhanced Traffic Offload:**
 - In this mode, Suricata's specialized rules assess and classify network traffic with greater precision, particularly when identifying encrypted communication. While Suricata still controls which flows are offloaded, it provides more granular instructions to the FPGA for improved traffic processing efficiency.
 - **CPU Core Savings:** Up to 40% reduction in CPU core usage due to more effective traffic filtering and decreased processing demands on the IDS.

- **FPGA-based TLS Offload:**
 - In this mode, the FPGA independently handles the identification and processing of encrypted TLS connections, ensuring that only essential data is forwarded to the IDS. While Suricata can still send bypass requests for general traffic management, the encrypted traffic offload is fully autonomous, allowing for seamless and efficient processing without CPU intervention.
 - **CPU Core Savings:** Up to 60% reduction in CPU core usage, allowing Suricata to manage vastly increased traffic volumes with fewer computational resources.

- **Full FPGA-based Offload:**
 - On top of the TLS bypass, Suricata receives per-packet metadata about matched patterns. DYNANIC's pattern-matching engine in the FPGA searches for Suricata-defined patterns. Matches are then noted as per-packet metadata.
 - **CPU Core Savings:** Up to 70% reduction in CPU core usage.

Performance Analysis

Studies conducted by CESNET show that DYNANIC significantly improves Suricata's processing capabilities. In 100 Gbps environments, DYNANIC reduces the CPU cores required for wire-speed IDS operation from over 150 to approximately 50, depending on the level of acceleration applied. Since real-world networks rarely operate at peak capacity, typical reductions range from over 75 cores to fewer than 25.

By lowering CPU requirements, DYNANIC allows IDS processing to be handled by fewer servers, leading to lower infrastructure costs and simplified management. Fewer servers mean reduced spending on hardware, power, and cooling while also decreasing the operational complexity of maintaining multiple systems.

Beyond resource optimization, DYNANIC improves detection accuracy by offloading traffic processing, which helps minimize false positives. Its ability to consolidate workloads into a single system makes IDS deployments more efficient and easier to manage. With fewer servers and lower operational overhead, organizations can achieve high-performance monitoring at a reduced cost.

Conclusion

DYNANIC, with its advanced hardware acceleration capabilities, represents a significant leap forward in the performance and efficiency of Suricata-based IDS systems. By reducing the dependency on CPU resources, DYNANIC allows organizations to scale their IDS deployments more effectively, ensuring robust network security even in high-speed environments.

The collaboration with CESNET has demonstrated the real-world effectiveness of this FPGA-powered solution, highlighting its potential to revolutionize the way organizations approach network intrusion detection. Whether through basic traffic bypass or full FPGA integration, DYNANIC offers a flexible and powerful solution for enhancing IDS performance and reducing operational costs.

Contact Information

DYNANICWebsite: www.dyna-nic.comEmail: info@dyna-nic.com**CESNET**Website: www.cesnet.czEmail: tmc-info@cesnet.cz