What is mCore?

- A vendor independent high-performance packet forwarding engine
- Runs on any DPDK-capable NIC, leverages DPDK high-performance features
- Forwards packets from the NIC to $N$ parallel applications, including Suricata and Zeek
- Suricata integration:
  - Utilizes multi-threaded workers for scalability
  - Easy configuration through suricata.yaml
  - Integrated with Suricata stats counters (packets, bytes, drops)

Base Architecture

- mCore controller: Initiates, manages, terminates the forwarding engine
- mcore-net-util: User CLI
- Plugins: Support for Zeek, Suricata, TAP
- Can filter traffic using DPDK rte_flow and BPF

High-Performance Optimizations

- Kernel bypass
- Zero packet copy
- Lockless data structures
- Intelligent packet shunting
- NUMA affinity
- CPU/core affinity/pinning
- Multi-core elastic scalability
- Selective packet capture

Base Architecture

- mCore controller: Initiates, manages, terminates the forwarding engine
- mcore-net-util: User CLI
- Plugins: Support for Zeek, Suricata, TAP
- Can filter traffic using DPDK rte_flow and BPF

High-Performance Optimizations

- Kernel bypass
- Zero packet copy
- Lockless data structures
- Intelligent packet shunting
- NUMA affinity
- CPU/core affinity/pinning
- Multi-core elastic scalability
- Selective packet capture