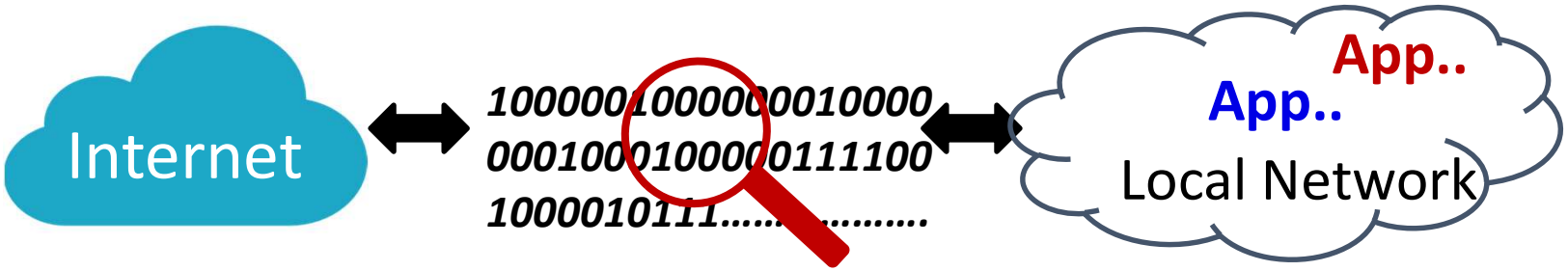
Pigasus: FPGA-Accelerated 100Gbps Network Intrusion Prevention

Zhipeng Zhao, Hugo Sadok, Nirav Atre, Minya Rancic,
James C. Hoe, Vyas Sekar, Justine Sherry
Carnegie Mellon University

with generous support from SRC/JUMP CONIX, Intel, and VMware

Intrusion Prevention System



- Check packet payload against a set (10s K) of elaborate rules (e.g., regular expressions)

  Data and compute Intensive

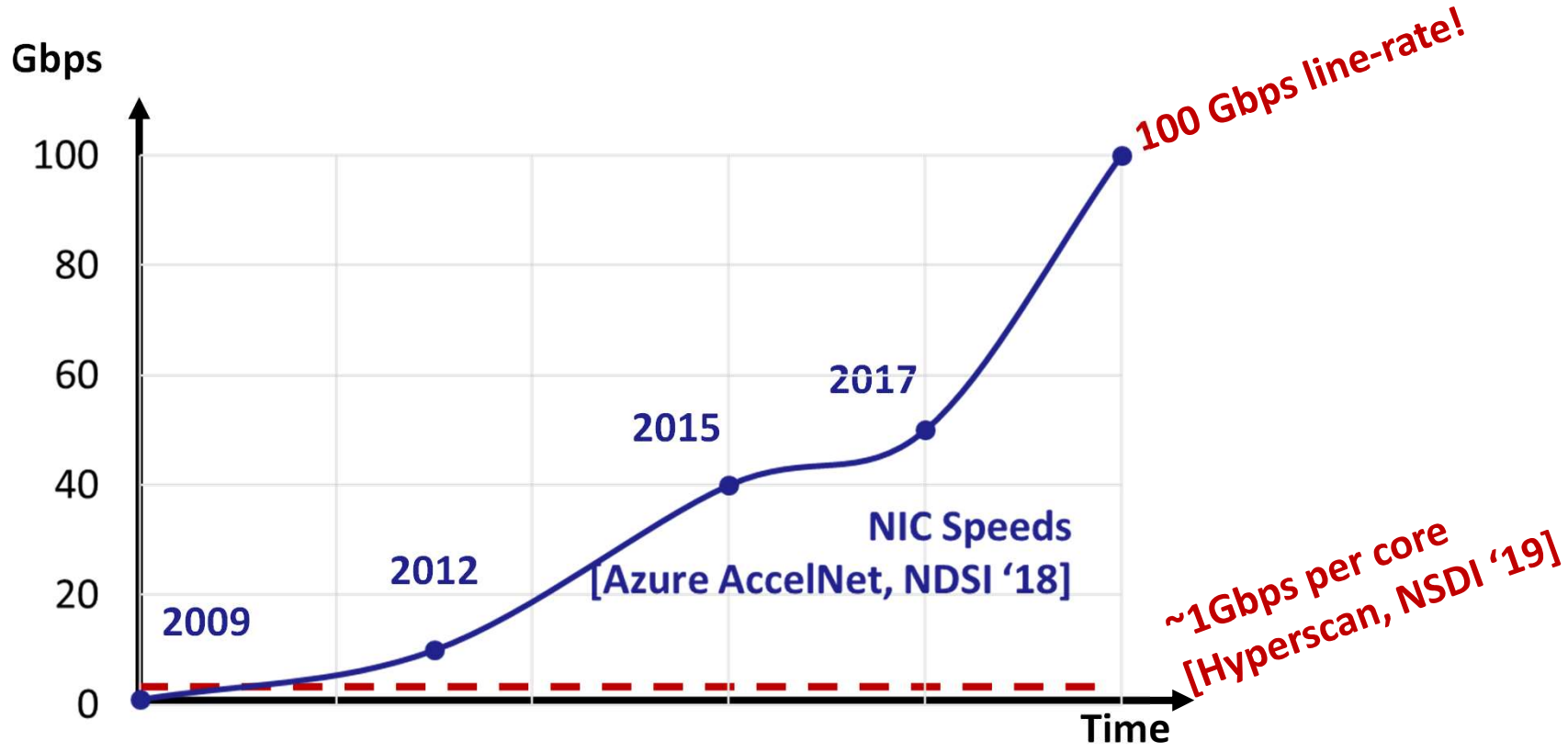
- Performed inline with traffic

  Must keep up with line rate

- Stop malicious packet from propagating

  Latency matters

Software State of the Art: SNORT 3.0 with Hyperscan

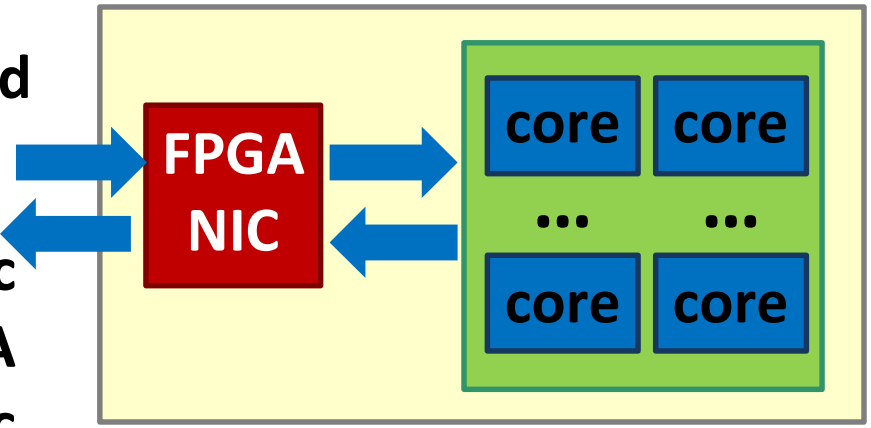


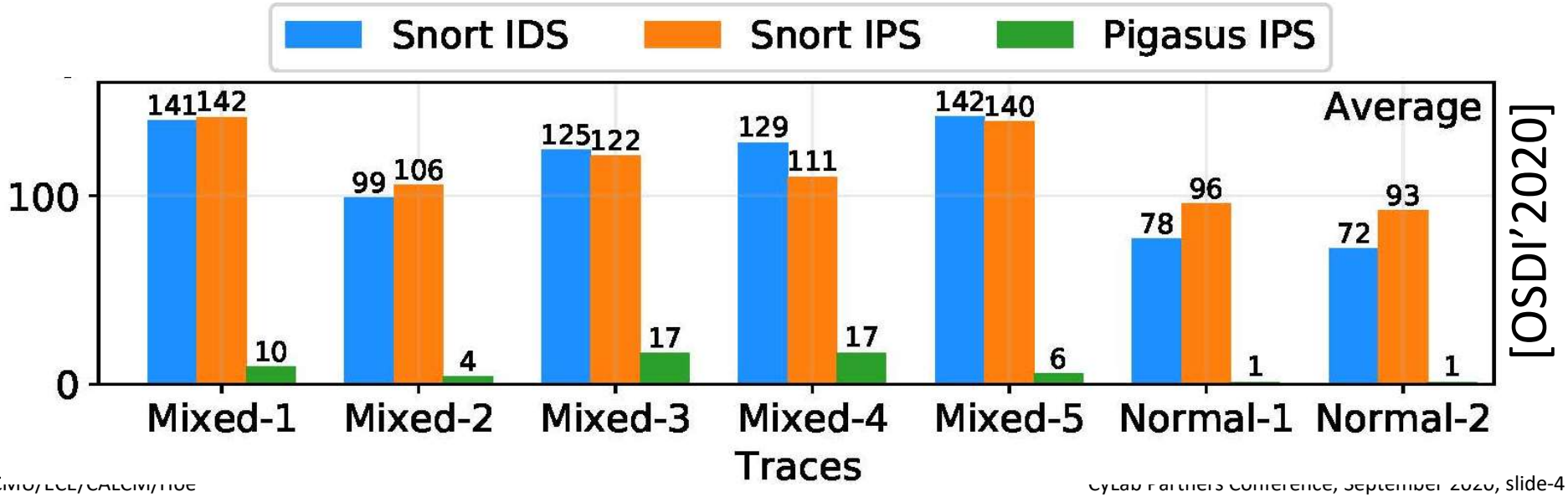
Split traffic by flows to scale onto 100 cores, or solve this with 1 FPGA

Pigasus 100Gpbs ID/PS (1 FPGA + 1 CPU)

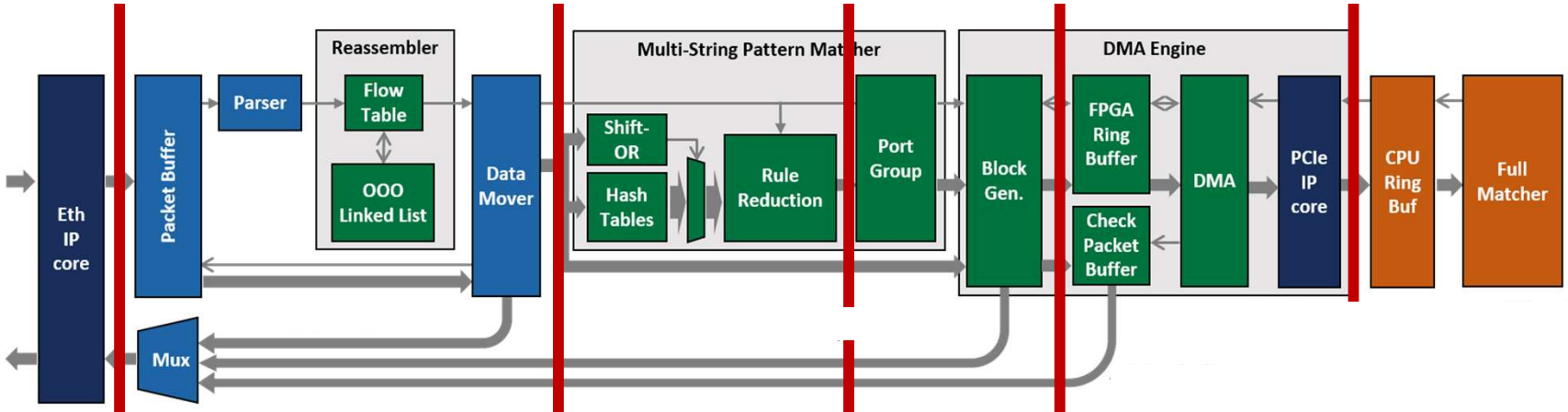
100Gbps inbound

90+% traffic cleared by FPGA under 5usec

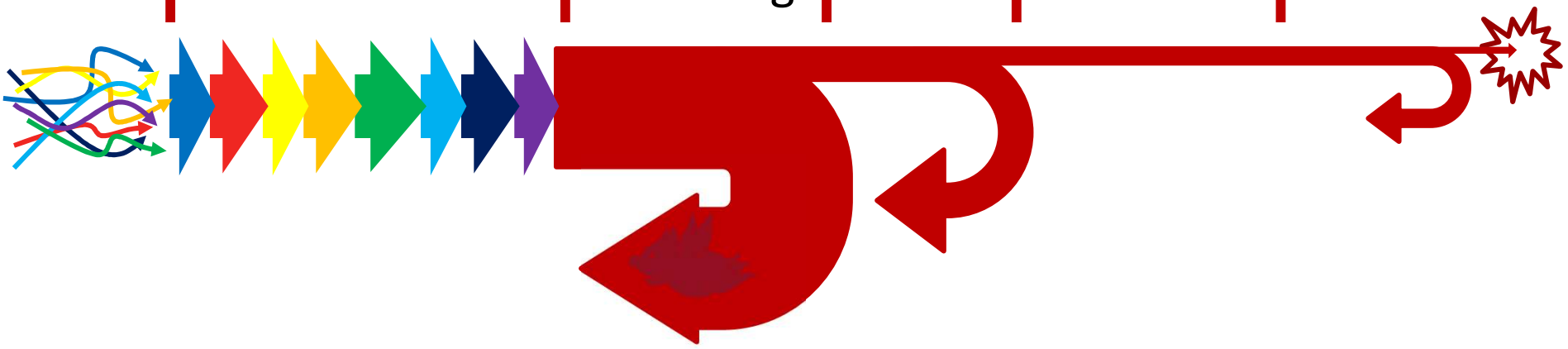




Pigasus: FPGA-First Architecture



ethrnt | TCP flow reassembly | "fast pattern" matching | 2nd filtering | Offloading to CPU | CPU full matching

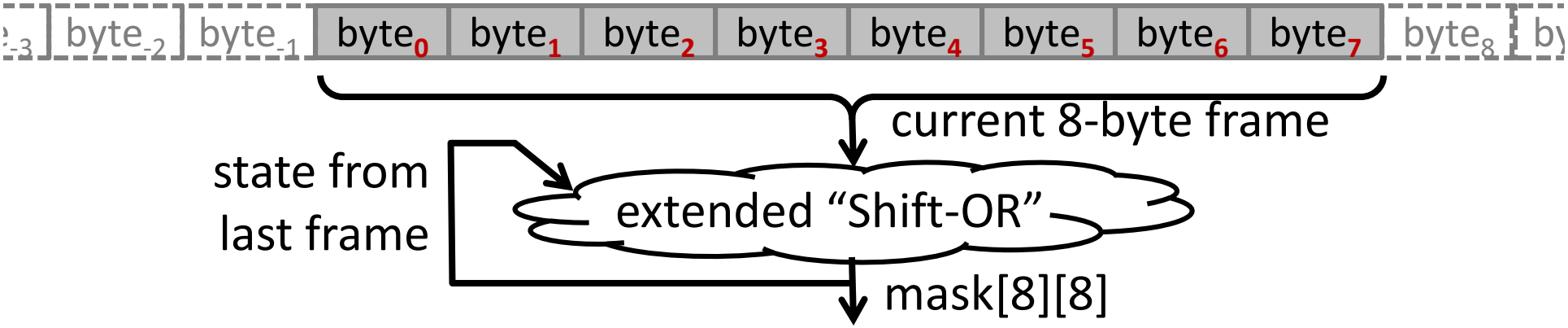


HW&SW open-sourced from here.

10s K ↘ Multistring Matching

- Hyperscan SSE/AVX parallel algo. [NSDI'2019]

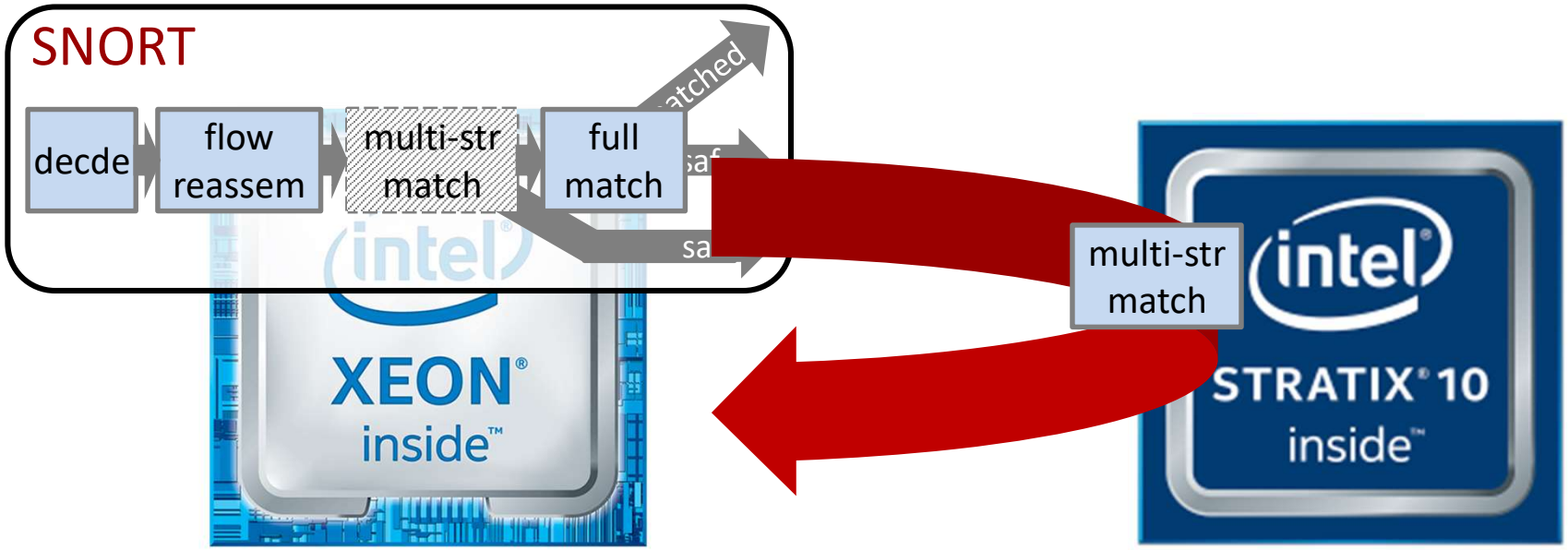
  improved 10x over prior art to 1Gbps/sec/core



- A problem inherently better suited for HW
  - unrolled Hyperscan algorithm 4 times
  - pipelined to process 32 bytes per cycle

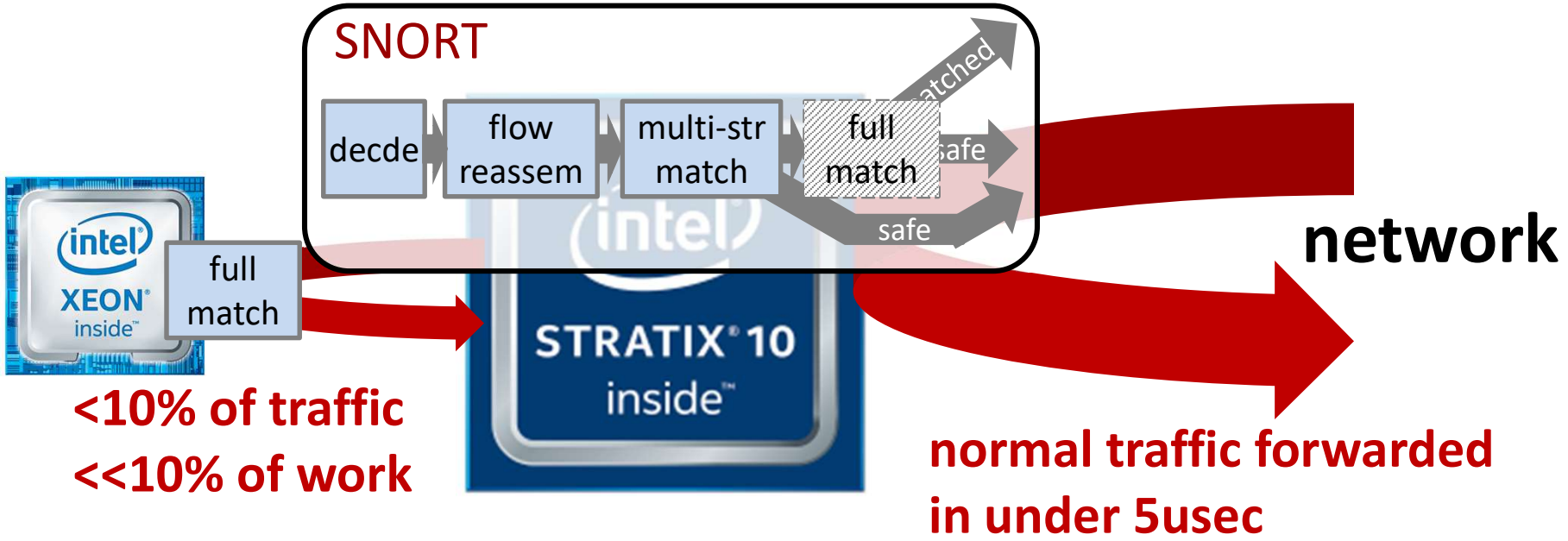
  102Gpbs@400MHz using ~20% FPGA

FPGA Offload Non-Solution



- Multiple PCIe crossings: NIC→CPU→FPGA → CPU→NIC
- In throughput applications, all stages need to be fast together

Putting FPGA in Front



- FPGA receives packets directly off the network
- Check "fast-pattern" to reject impossible matches (safe) and forward out immediately
- Offload potential matches to CPU for full check (mostly false positives in practice)

Conclusion

- IPS at 100Gbps (and more) on 1 FPGA demonstrated and open sourced

  Read on github here.

- Reproducing 100% SNORT functionality still hard
  - years of accumulated features and optimizations
  - inactive binary is free, but inactive logic still costs

  HW and SW are different

- Question: what to do with 100x . . .

When IPS is 100x cheaper . . .