DYNANIC

Silicom Denmark A/S FPGA SOLUTIONS

Experience Unmatched Network Efficiency and FPGA Excelence

Accelerating Anti-DDoS systems

Problem statement

As the number of Distributed Denial of Service (DDoS) attacks increases, there is a need to build faster and smarter mitigation systems. Especially in the case of volumetric DDoS attacks, **hundreds of thousands of attackers need to be filtered to protect the network infrastructure.**

The filtering tables in core routers do not have enough capacity for filtering rules and sometimes do not have enough performance. Software-driven Anti-DDoS solutions lead to high latency, excessive resource (CPU) consumption, and limited scalability in protecting high-speed network infrastructure. ASIC-based hardware solutions lack flexibility and cannot adapt to evolving attack patterns, making them ineffective against sophisticated threats.

DYNANIC delivers DDoS mitigation without CPU bottlenecks, reducing latency, and enhancing flexible attack detection accuracy while significantly cutting infrastructure costs.

Solution description

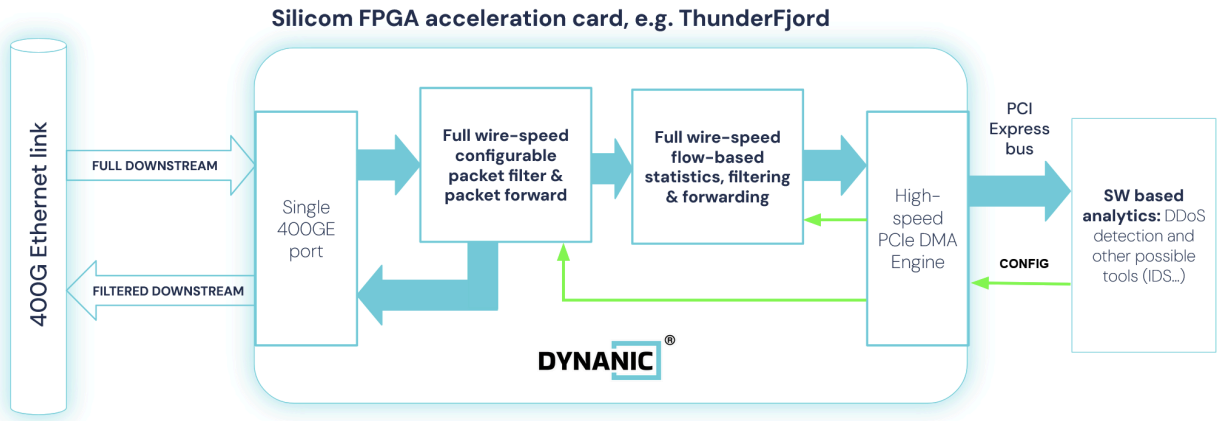
DYNANIC offers an efficient solution for mitigating distributed denial-of-service (DDoS) attacks directly at the hardware level by integrating Silicom's FPGA SmartNICs. Incoming network traffic is processed through a programmable pipeline implemented on Silicom's high-performance FPGA cards, such as the Silicom ThunderFjord (FB2CDG1@AGM series), N6010, or FB2CG(HH)@KU15P SmartNICs. This pipeline performs multi-stage filtering and intelligent forwarding, with mirrored traffic optionally delivered to the host system, where traffic analysis in software oversees the entire DDoS mitigation process.

For more information visit
www.dyna-nic.com and www.silicom.dk

The DDoS mitigation scenario is based on two coordinated processing stages within the DYNANIC unique pipeline:

- **Hardware Filtering and Forwarding:** The first stage of the FPGA pipeline performs hardware-based filtering and forwarding of network traffic. Suspicious or known-malicious packets are dropped based on blacklists or heuristic rules, ensuring that harmful traffic is blocked early. Trusted and verified traffic is forwarded directly to the output interface, bypassing the host entirely to ensure minimal latency for legitimate flows.
- **Statistics and Flow-Based Analysis:** To enhance decision-making, full wire-speed network traffic statistics are calculated in the second stage, and then selected flows are mirrored to the host system for software-based traffic analysis. The software typically inspects just the first N packets of a flow. If the flow is deemed legitimate/malicious, the update of the whole FPGA pipeline is made on the fly, allowing subsequent packets of the same flow not to be forwarded to the CPU to protect its overload.

These two tightly integrated stages ensure fast reaction to threats and **optimal performance for clean traffic, leveraging both the speed of hardware and software adaptability.** This hybrid approach combines **ultra-low-latency packet handling (under 1 microsecond) with the flexibility of software-defined intelligence.** The entire mitigation strategy is controlled through a standard software API based on the DPDK RTE Flow interface — no hardware development tools or FPGA knowledge are required!



Key Advantages

- **Real-Time Inline Mitigation & Ultra-Low Latency:** Processes DDoS attack filtering in hardware, reducing response times by 80% and enabling 400Gbps+ line-rate mitigation without affecting legitimate traffic.
- **Scalable & Adaptive Protection:** Unlike CPU-based solutions, Silicom FPGA SmartNIC with DYNANIC can dynamically adapt to new attack patterns, enabling programmable rule sets, AI-driven threat detection, and real-time updates to counter evolving threats.
- **Massive CPU Offload & Infrastructure Efficiency:** Offloads DDoS filtering from CPUs, reducing CPU utilization by 50-80% and enabling lower server counts, reducing CAPEX and OPEX while maintaining network performance.
- **Inline Packet Inspection & Filtering:** Performs deep packet inspection (DPI), flow-based behavioral analysis and detection, and rate-limiting, blocking malicious traffic before it reaches critical infrastructure.
- **Lower Total Cost of Ownership (TCO):** DYNANIC, together with Silicom FPGA HW ensures that the higher upfront costs associated with FPGA technology are recovered, as it reduces the server requirements, lowering power consumption, extends hardware lifespan, delivering cost-efficient, high-performance DDoS protection over 5-7 years.

Value for Customers

The acceleration of Anto-DDoS systems delivers tangible benefits for telecommunications operators and data center infrastructure providers:

- In telco networks, extremely low-latency hardware forwarding ensures real-time response to network events while dramatically reducing CPU load on host systems. This **allows operators to process high traffic volumes at the network edge without overprovisioning compute resources,** leading to more efficient and cost-effective deployments.
- In data center environments, the solution enables consolidation by offloading traffic processing from CPUs. Depending on the specific scenario, this **reduces the number of required servers by up to 50%, directly cutting both CAPEX and OPEX,** including energy consumption and rack space.

DYNANIC

Silicom Denmark A/S FPGA SOLUTIONS

Experience Unmatched Network Efficiency and FPGA Excelence

Overall, a commodity server with multiple 100GbE or even 400GbE capable Silicom FPGA SmartNIC loaded with DYNANIC is an extremely powerful yet flexible enabler for Anti-DDoS solutions in data centers.

Feel free to contact us at:

info@dyna-nic.com or contactus@silicom.dk

For more information visit
www.dyna-nic.com and www.silicom.dk