DYNANIC

Experience Unmatched Network Efficiency
www.dyna-nic.com

Use-case: *Anti-DDoS acceleration*

Problem statement

As the number of Distributed Denial of Service (DDoS) attacks increase, 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 power.

Solution description

DYNANIC provides low latency and high throughput, while saving the CPU cores idle for the application. Moreover, it can run on virtually any FPGA-based card from a host of major high-end hardware manufacturers. Overall, **a commodity server with multiple 100GbE or even 400GbE capable FPGA-card(s) loaded with DYNANIC** is an extremely powerful yet flexible solution to support acceleration of any Anti-DDoS solution.

Main features

- Network traffic processing with low-latency and wire-speed throughput
- Large filtering and forwarding tables with up to 500k unique rules
- Customisation of matching parameters based on individual requirements
- Up to 64 general flow rules for wire-speed packet capture (forensic analysis)
- Flow level statistics for incoming traffic and counters for all filtering rules

BRNO LOGIC

BrnoLogic offers custom design and development services for FPGA-based projects. For more than 20 years the company team members are specializing in the acceleration of algorithms required for high-speed network packet processing (e.g. packet parsing, packet/headers fields extraction, hash based pattern matching, filtering, traffic flow management, etc.). Unique portfolio of IPs for link speeds of up to 400 Gbps was also utilized to bring FPGA technology closer to any customer, where network efficiency matters. That's how **DYNANIC** solution was created.