Packet Classification for Anti-Distributed Denial of Service (DDoS) Engines – Combining AI/ML with ACL Lookups

Use Case

KEY CHALLENGES:

It never ceases to amaze how creative the criminals that institute Distributed Denial of Service Attacks (DDoS) can get. Gone are the days that a simple Syn Flood attack is all that they will throw at you – now much more complex attack vectors are in play – all designed to use up precious networking and server resources and either bring performance to its knees or perhaps open up some buffer overload attack sequence.

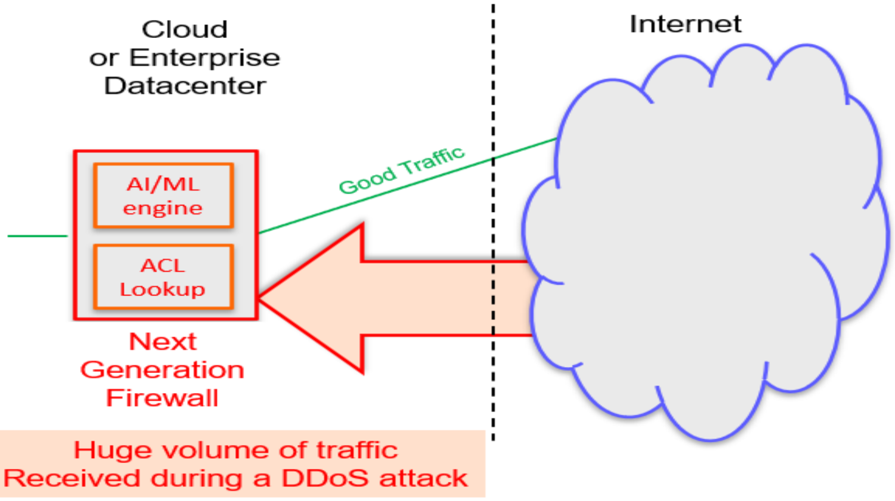
Anti-DDoS engine complexity has increased dramatically in the last decade – now they often include some form of Artificial Intelligence or Machine Learning Algorithms to help spot DDoS attacks, but typically the first and last stages still use Access Control list lookups which can become an overall bottleneck. Allow/Deny Lists can contain tens of millions of rules.

As a packet from a new flow is established it is the responsibility for the Anti-DDoS engine to decide whether to grant entry into the network – to do this it can lookup various information to decide if this flow is from a known bad actor – typically one of the first gates to pass through is the Access Control List (ACL) lookup – these can involve very complex multiple tuple lookups that dive deeply into the packet headers – the term Deep Packet Inspection (DHI) is now being applied to such lookups and is a kindred spirit to Deep Packet Inspection (DPI) that examines the payload of the packet.

Once an AI system decides that a set of header parameters indicates malware it will quickly update the ACL table so that precious AI resources are not wasted.

Strong Security requires that the headers of each packet are examined in real-time, this can use a combination of Exact Match, Longest Prefix Match (LPM) and Access Control List match (ACL).

Depending on the system, the total number of rules, the number of rules that match, the complexity of the rules and the speed of the searches (Millions of searches per sec) determine the overall performance level.



Packet Classification for Anti-Distributed Denial of Service (DDoS) Engines – Combining AI/ML with ACL Lookups

Use Case

KEY SYSTEM CONSIDERATIONS:

- Anti-DDoS engines sit at the edge of the datacenter or major corporate networks.
- There is a growing interest to also add Anti-DDoS engines to every server
- Growing SmartNICs/DPU usage for Anti-DDoS
- Require the ability for an AI /ML system to do extremely fast ACL rule updates
- Typical 100K – 50+ Million very complex rules at 50 – 400+ Million searches per second
- Typical 100Gbps to Terabits/s with low latency a must

Meeting the search requirements can be accomplished in several ways:

- Execution in Software – but this can be too slow
- Using a standalone TCAM chip – but this can be high cost and high power
- Using a hardware accelerated Algorithmic TCAM in ASIC or FPGA
- Combining a multi-terabit SmartSwitch with any of the above

MOSYS SOLUTION

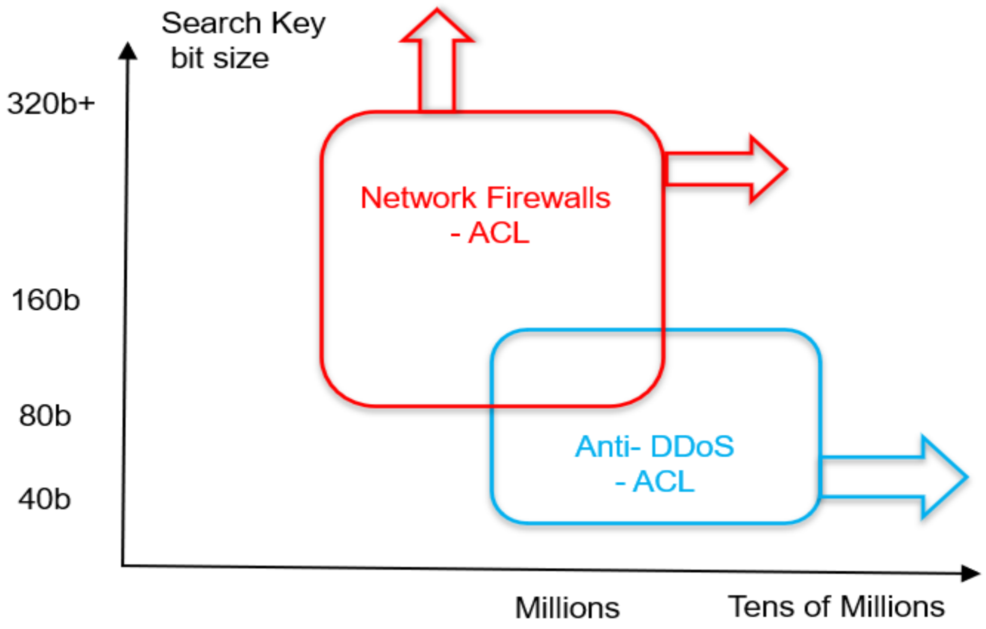
The MoSys Stellar Packet Classification Platform – High Flexibility/High Complexity ACL & LPM are provided as Intellectual Property (IP) that uses a hardware accelerated Algorithmic TCAM-like approach to help ensure that Anti-DDoS engines can keep up with the huge volume of access control decisions per second that it has to process.

High Flexibility/High Complexity ACL & LPM

- Ultra-High-Speed Search Engine IP
- Deep Header Inspection (DHI) solution
- Available for ASIC or FPGA
- Optimized for high performance security
  - Ideal for anti-DDoS engines
  - Can add other functions
  - Firewall, routing, load balancing
- Tuned for Access Control List (ACL)
  - Optimized for up to 10 tuple matches
  - Also supports Exact Match and LPM
  - Can also support routing lookups
- Provides scalable performance
  - Uses Graph Memory Engine (GME)
  - 100s of Million lookups per second
  - Low latency solution
  - Very efficient memory usage
  - Extremely efficient use of logic gates
  - Very fast rule updates
  - No need to recompile rules
  - No need to preconfigure table sizes
  - On the fly updates – no need to stop traffic
  - Ability to receive updates from AI/ML logic
  - Supports large number of bits for next hop data
  - Capacities and key sizes beyond normal routing
  - Up to multigigabit TCAM equivalence
- **Supports broad range of devices**
  - Can utilize hybrid mix of memories
  - Internal SRAM and/or external DDR, HBM
  - Can also use MoSys memories, but can operate without any MoSys silicon present
  - Supports RTL for Intel Stratix 10, Xilinx UltraScale+ FPGAs, or ASIC/SoC/DPU…
  - Replaces multiple expensive and power hungry TCAM chips
  - Common API for software interface – easier to port applications
  - Applicable to designs based on NIC, SmartNIC, DPU, Standalone SoC, SmartSwitch…

KEY POINTS SUMMARY:

- Very High-Performance solution designed to accelerate one of the main Anti-DDoS bottlenecks – complex multi-tuple access control lookups
- Very flexible design – MoSys IP easily integrated
- Takes advantage of available gates and memory in FPGA or ASIC
- Helps future proof designs by supporting wide range of key sizes, n+ tuple looks ups, very large number of rules at a very high performance in very efficient logic



ADDITIONAL RESOURCES:

Stellar Virtual Acceleration Engines
Stellar Virtual Acceleration Platform
Virtual Acceleration: The MoSys Approach
Cheetah Development Kit