Packet Classification for Next Generation Network Firewalls Combining AI/ML Engines with ACL Lookups

Use Case

KEY CHALLENGES:

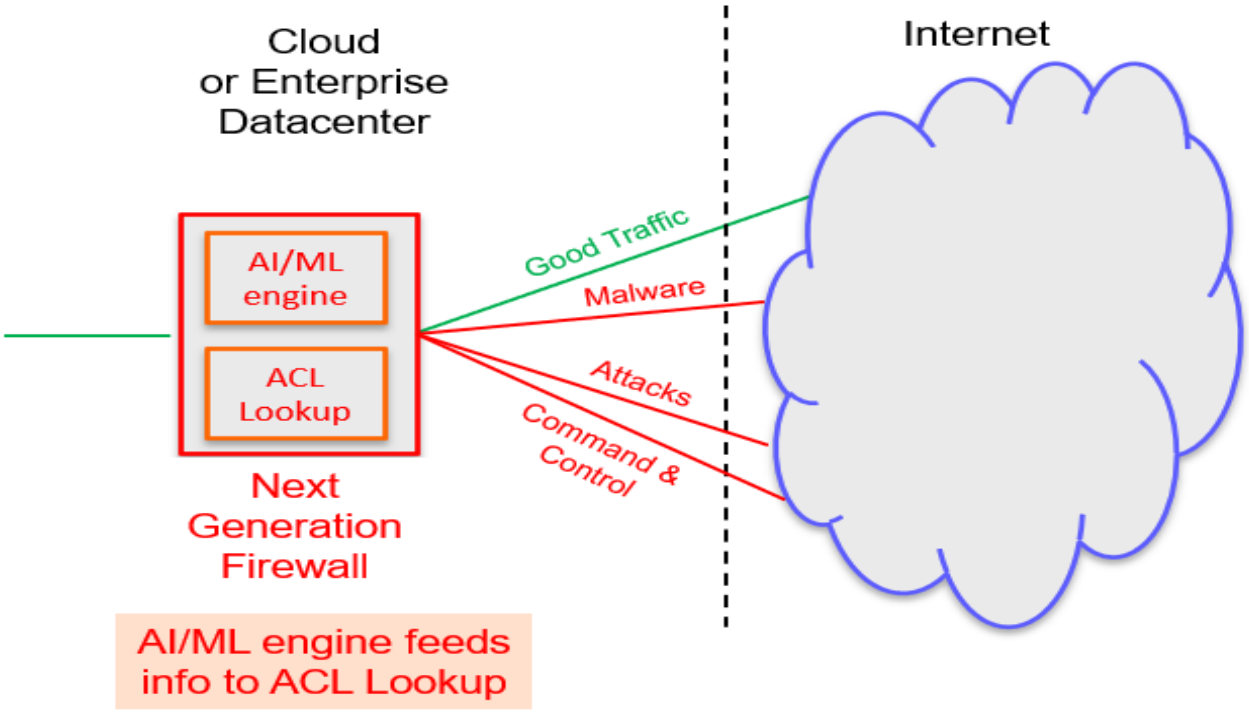
Network Firewalls complexity has increased dramatically in the last decade – now they often include some form of Artificial Intelligence or Machine Learning Algorithms to spot malware infestations, but typically the first and last stages use Access Control list lookups which can become an overall bottleneck.

As a packet from a new flow is established it is the responsibility for the Network Firewall to decide whether to grant entry into the network – to do this it can lookup various information to decide if this flow is from or know 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 given set of header parameters indicates malware it will quickly update the ACL table so that precious AI resources are not spent on coming to the same decision.

Strong Security requires that the headers of each packet be 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 Next Generation Network Firewalls Combining AI/ML Engines with ACL Lookups

Use Case

KEY SYSTEM CONSIDERATIONS:

- Next Gen Network Firewalls (NGFW) sit at the edge of the datacenter or major corporate networks.
- There is a growing interest to also add a network firewall to every server in the data center – SmartNICs/DPU are being pressed into service for this
- Deep Packet Header Inspection requirements - require millions of rules and the ability for an AI /ML system to do extremely fast rule updates
- Typical 100K – 1+ Million very complex rules – examines VLAN tags as well
- Typical 50 – 150+ 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 Smart Switch 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 Network Firewalls can keep up with the huge volume of access control decisions per second that it has to process.

High Flexibility/High Complexity ACL & LPM

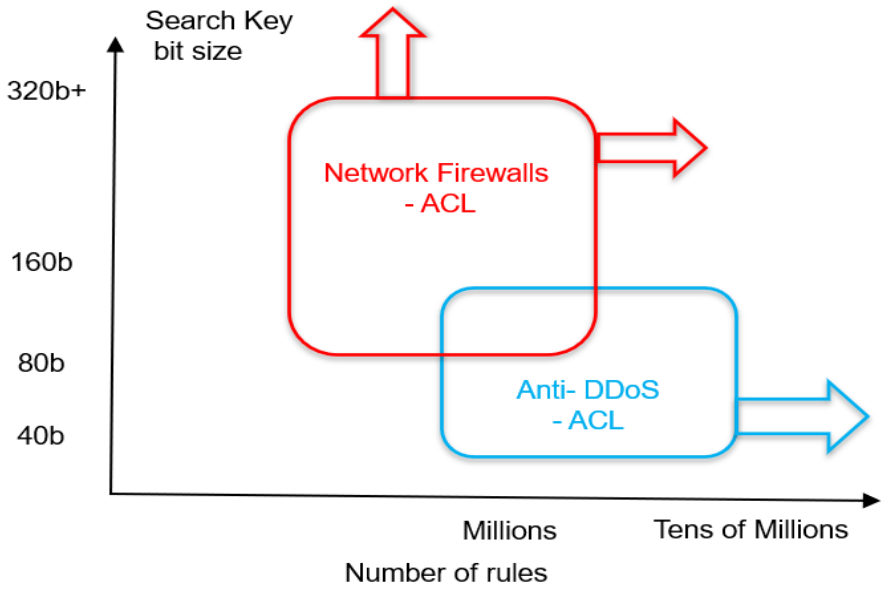
- Ultra-High-Speed Search Engine IP
- Deep Header Inspection (DHI) solution
- Available for ASIC or FPGA
- Optimized for high performance Security
  - Ideal for Next Gen Firewalls (NGFW)
  - Can add other functions
  - Anti-DDoS, Routing, load balancing…
- Tuned for Access Control List (ACL)
  - Optimized 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
  - Up to multi-gigabit 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…

Packet Classification for Next Generation Network Firewalls Combining AI/ML Engines with ACL Lookups

Use Case

KEY POINTS SUMMARY:

- Very High-Performance solution designed to accelerate one of the main Network Firewall 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

2309 Bering Drive, San Jose, CA 95131
Tel: 408-418-7500

Document No:
PacketClassNextGenNetworkfirewalls_20210617