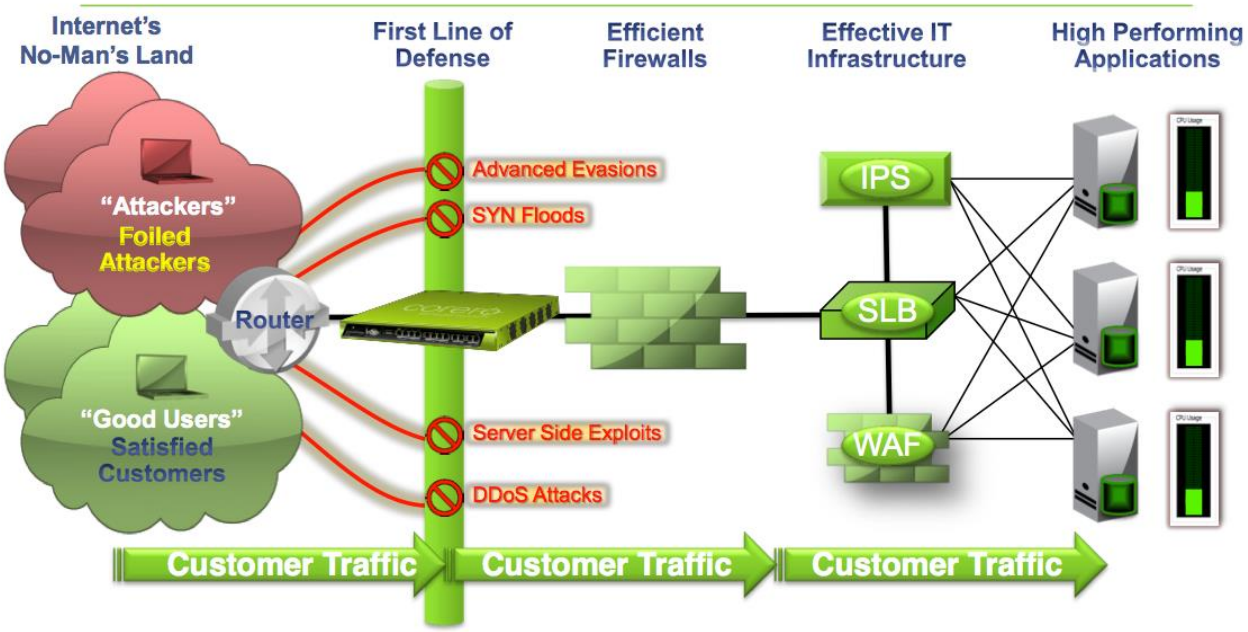
Early DDoS Attack Detection by a Stateless Device

Abstract:

Detecting Distributed Denial of Service (DDoS) attacks by the router or the switch located in early stage before the attacked server can improve significantly the overall performance since the switch/router itself can trigger packet based filtering rules in order to reduce the load towards the servers.

A good sign for DDoS attack is an increasing or high rate of active flows in each time slot – compared to normal or pre-defined number of flows threshold. In order to detect such case – it is required from a stateless device to be able to estimate on-line the total number of flows while using small memory footprint. The number of flows estimation can be done by working and analyzing the entire stream or only on a sampled stream.



Goals:

Implement real-time DDoS attack detection in a stateless device (Router/Switch) in 2 ways:

a. Analyzing the entire stream: Estimate the number of flows in each time slot (For example: in 30 seconds) by classifying each packet's 5-Tuple fields -using HyperLogLog algorithm with different number of memory buckets.
b. Analyzing sample of the stream: Estimate the number of flows in each time slot (For example: in 30 seconds) by classifying only sample packet's 5-Tuple fields -using HyperLogLog algorithm according to ***Cardinality Estimation Meets Good-Turing*** article (Algorithm 1)

Use ns-3 or mininet to simulate the topology with many hosts attackers, a stateless switch/router device and a server that will hold the connections. Generate DDoS attack by opening a high rate of flows (TCP, UDP) using DDoS tools or by injecting real captured traffic with DDoS attacks in it.
Compare the estimation accuracy resulted in each of the 2 methods.

Requirements:

Internet Networking Course

Guided by: