DDoS mitigation at 100G

Martin Žádník
CESNET, a.l.e.
Zikova 4, Prague

zadnik@cesnet.cz

Keywords. DDoS, detection, mitigation, protector, 100Gbps

Abstract

The volume of DDoS attacks grows every year. In 2016 the largest attacks reached 1 Tbps, effectively disconnecting even well provisioned services from the Internet. DDoS attacks are not only aimed at big players but smaller services and organizations are targeted with less intense, but effective enough, attacks as well. Unfortunately, the smaller players often lack budget and expertise to introduce adequate protection. CESNET is addressing this shortcoming by developing its custom DDoS protection device - DDoS Protector. The device consists of an 100 Gbps FPGA network card and a commodity server. The FPGA implements the fast forwarding and filtering data plane while the server implements the control plane that continuously evaluates the network traffic parameters and in case of attacks, it enables FPGA filtering with less than one second delay.

Under normal network conditions the Protector does not drop any packets. Only when DDoS traffic is detected the Protector starts to work as a filter. The goal of the filter is to drop DDoS packets to decrease the amount of traffic below an optimal limit. The Protector follows rules given by an administrator to behave deterministically. During configuration phase, an administrator defines a set of DDoS rules per each protected network prefix. The DDoS rule consists of conditions, limits and optimal traffic rate. The conditions specify which packet can match the rule (for example destination IP address must match IP prefix and dst port number of the packet must match dst port number in the rule). Limits specify the number of packets/s or bytes/s that must be exceeded to detect DDoS traffic targeting given IP prefix. Optimal traffic rate specifies the desired number of bytes/s or packets/s the DDoS traffic should be reduced to. The Protector evaluates rules upon user-defined periodic observation window.

Current mitigation is focused on reflection attacks where the IP address is not spoofed. In such a case those IP addresses that contributed the most to exceeding the threshold are selected for mitigation, the packets containing these IP addresses are dropped. However, the Protector offers an interface to implement other mitigation algorithms, for example, we develop a heuristic approach to mitigate TCP SYN flood attacks and our future work is to further extend mitigation algorithms to allow for their flexible utilization according the current attack surface.

Acknowledgment

This work was supported by the “CESNET E-Infrastructure” (LM2015042) funded by the Ministry of Education, Youth and Sports of the Czech Republic.