Protector: DDoS mitigation at 100G

Viktor Puš, Jan Kučera, Martin Zadnik, Jan Kořenek
(pus,jan.kucera,zadnik,korenek@cesnet.cz)

Motivation
- DDoS-for-hire industry
- Booters/Stresser service
- High volume attacks reaching 1 Tbps
- IoT – Mirai, but classy amplifications as well
- Small services and organizations need protection as well

Protector
- **Server with FPGA network card**
- Server acts as a control plane
- Card serves as a fast data plane
- No packet loss
- Microsecond delay
- Full IPv6 support
- Deterministic behavior

Architecture
- Attack is detected by network behavioral anomaly system
- All traffic to victim is forwarded to DDoS Protector utilizing BGP FlowSpec
- Protector identifies attackers
- Filtration takes place
- Filtered traffic is forwarded to the target

Deployment
- Connected to the neighbor router
- 1x 100GE, 10x 10GE interface
- Full IPv6 support
- VLAN mapping support
- Deployed at CESNET backbone

This research has been supported by the “CESNET Large Infrastructure” project no. LM2010005 funded by the Ministry of Education, Youth and Sports of the Czech Republic.