BUILDING OUR OWN DDOS PROTECTION AT 100 GBPS

Pavel Benáček, L. Kekely, M. Žádník

CESNET

INTRO

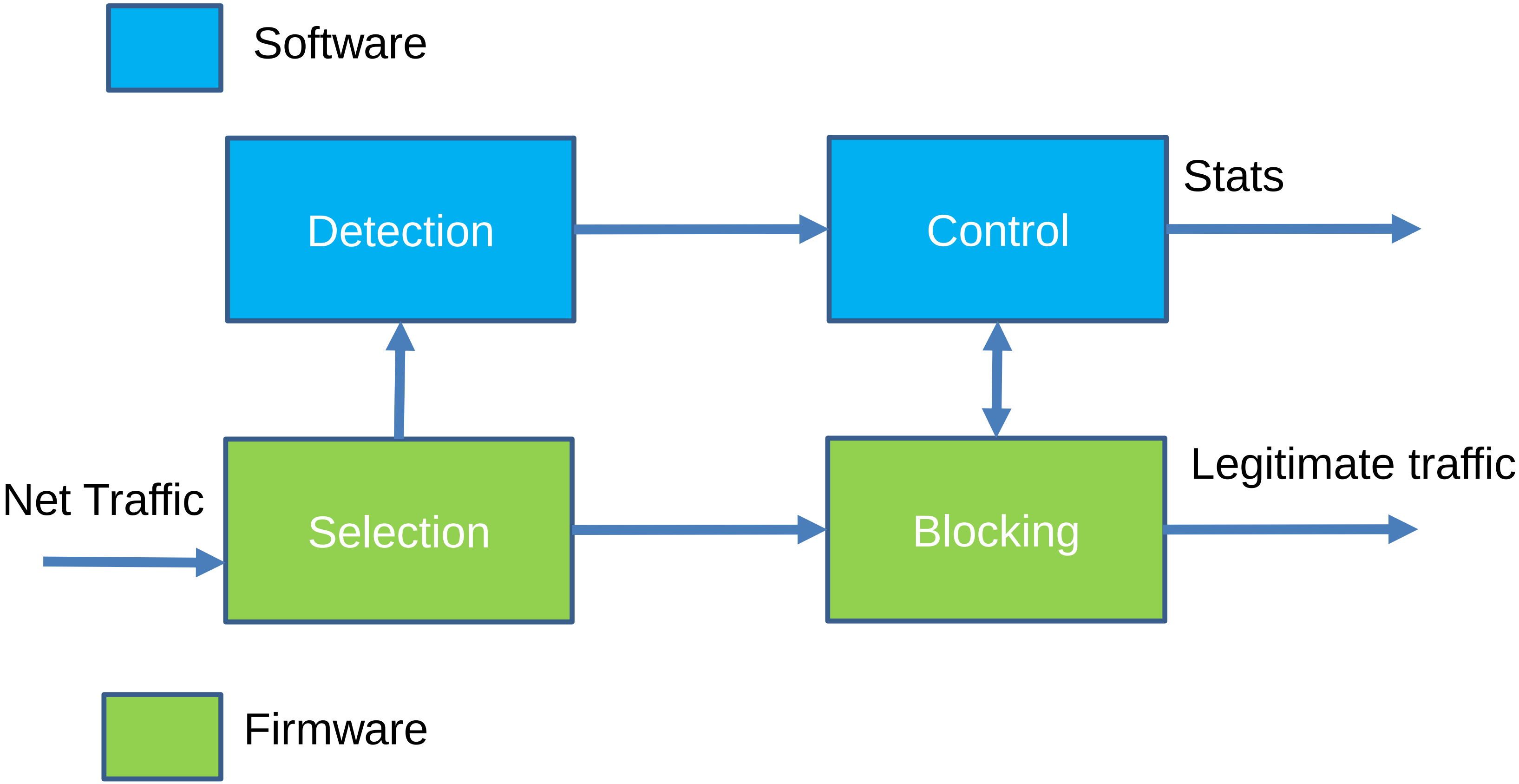
- **Why DDoS?**
  - Provider must deal with threats to infrastructure (including last mile)

- **Why on our own?**
  - More fine grained – rate limiting at routers is not good enough
  - Customizable
    - Specific needs
    - No need to wait for features in the roadmap
  - Order of magnitude cheaper but development must be accounted for

HOW?

- **DDoS mitigation device consists of**
  - Network card with programmable FPGA
  - Own firmware into FPGA
  - Own software running in a decent server

ARCHITECTURE



FEATURES

- Wire speed throughput 100Gbps
- Extremely low latency (microseconds)
- Support IPv6
- TCP flags
- Fragments
- Configuration: Linux interface + rules

LESSONS LEARNED

- **Deal with how to deploy**
  - Support of VLAN translation
  - Support of routing
  - Support of ARP, ND

- **Utilize what is already available**
  - BIRD, Suricata (to be utilized)

- **Practical and straight-forward approach usually works well**
  - Single-direction only
  - Heuristics to deal with various types of attacks

PLANS

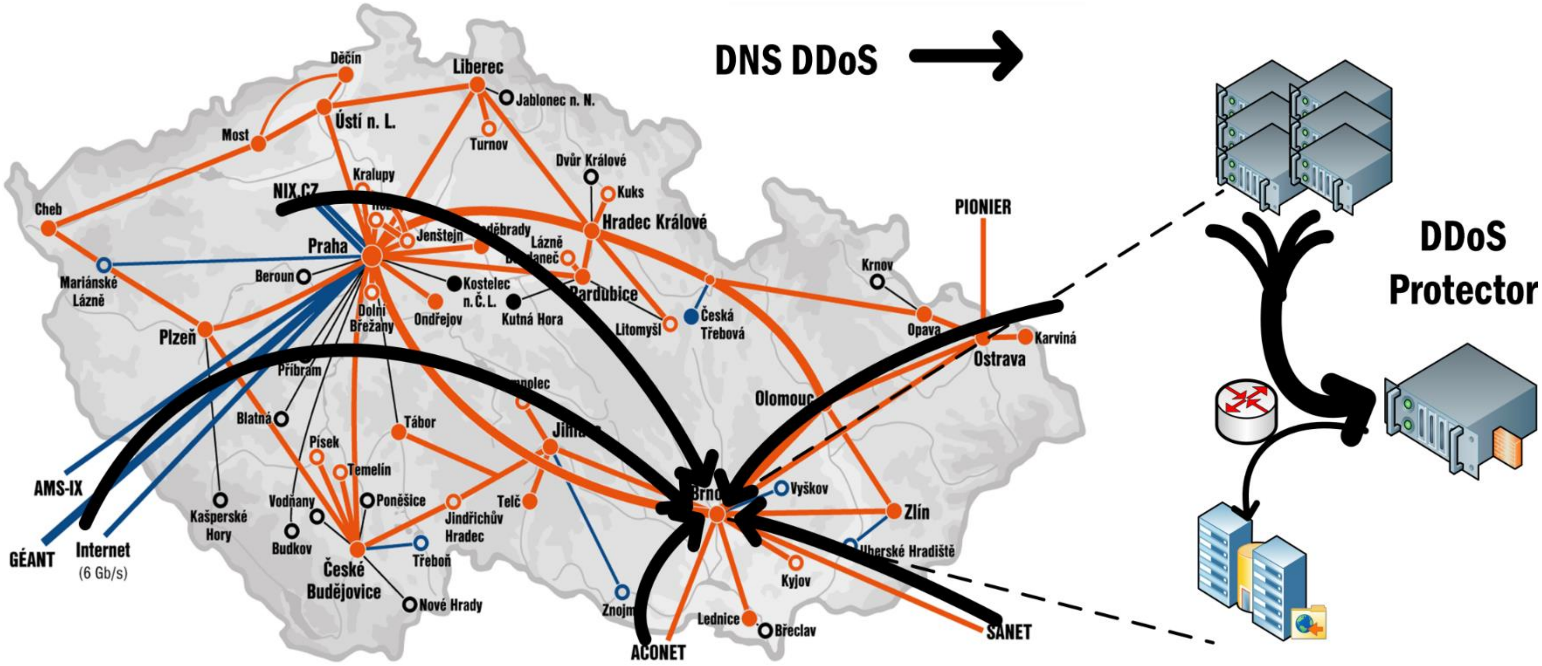
- **Extended blocking capacity**
- **Support various heuristics**
- **Build less proprietary interface**
  - BGP FlowSpec
  - Cisco-like CLI
- **Release**
  - Polish it till anyone can use it
  - Offer to others

cesnet

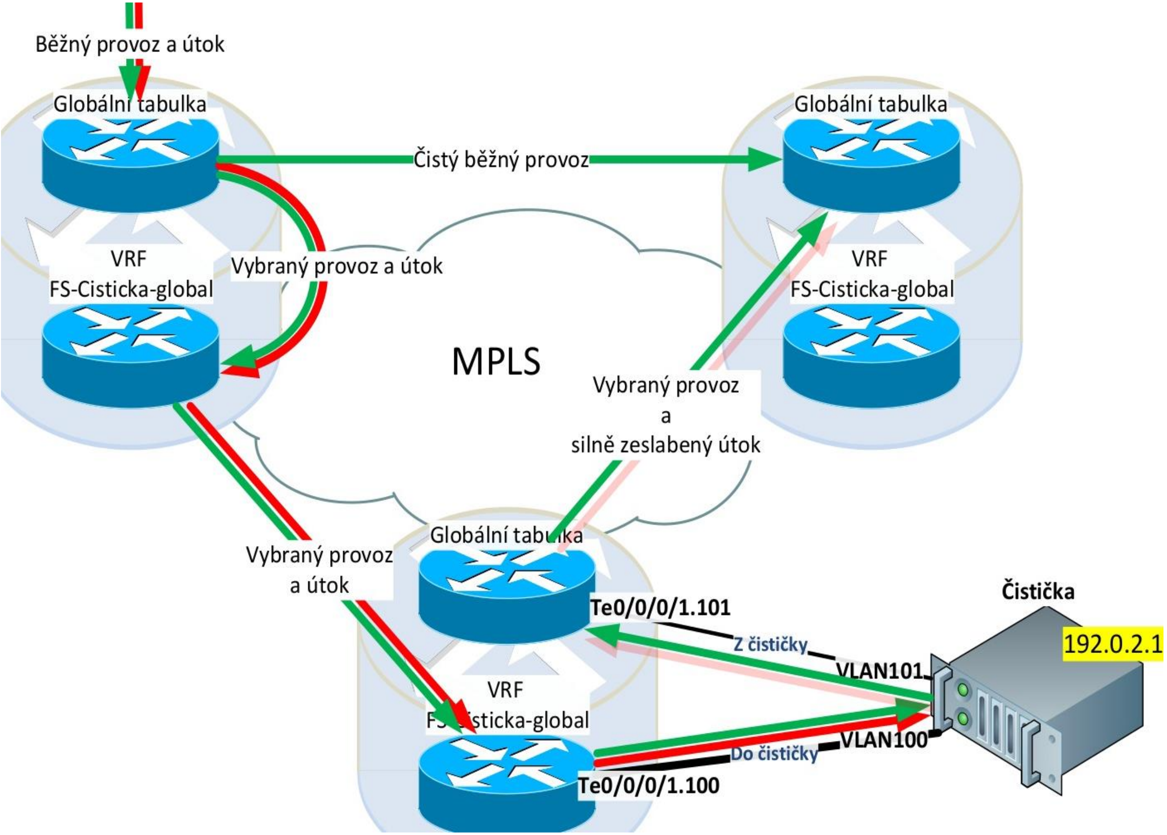
THANK YOU FOR YOUR ATTENTION

TRAFFIC REDIRECTION

- Forward suspicious traffic to Protector
- Return cleansed traffic to target destination

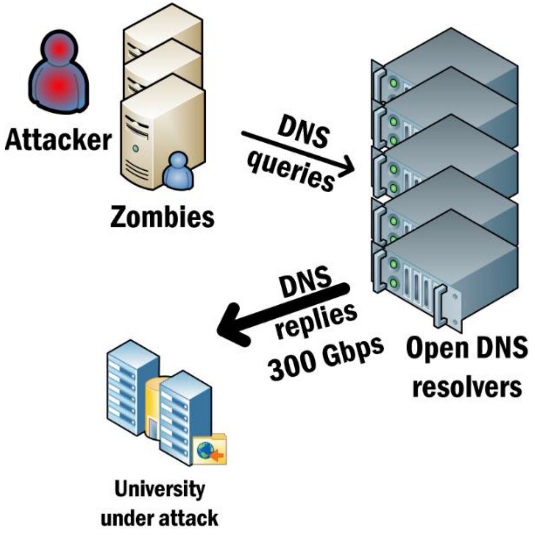


DETAILED REDIRECTION



ATTACKS OF INTEREST

- **Large reflection attacks**
  - DNS
  - NTP
  - LDAP
  - SSDP
  - SNMP
  - CharGEN



- **TCP SYN flood**