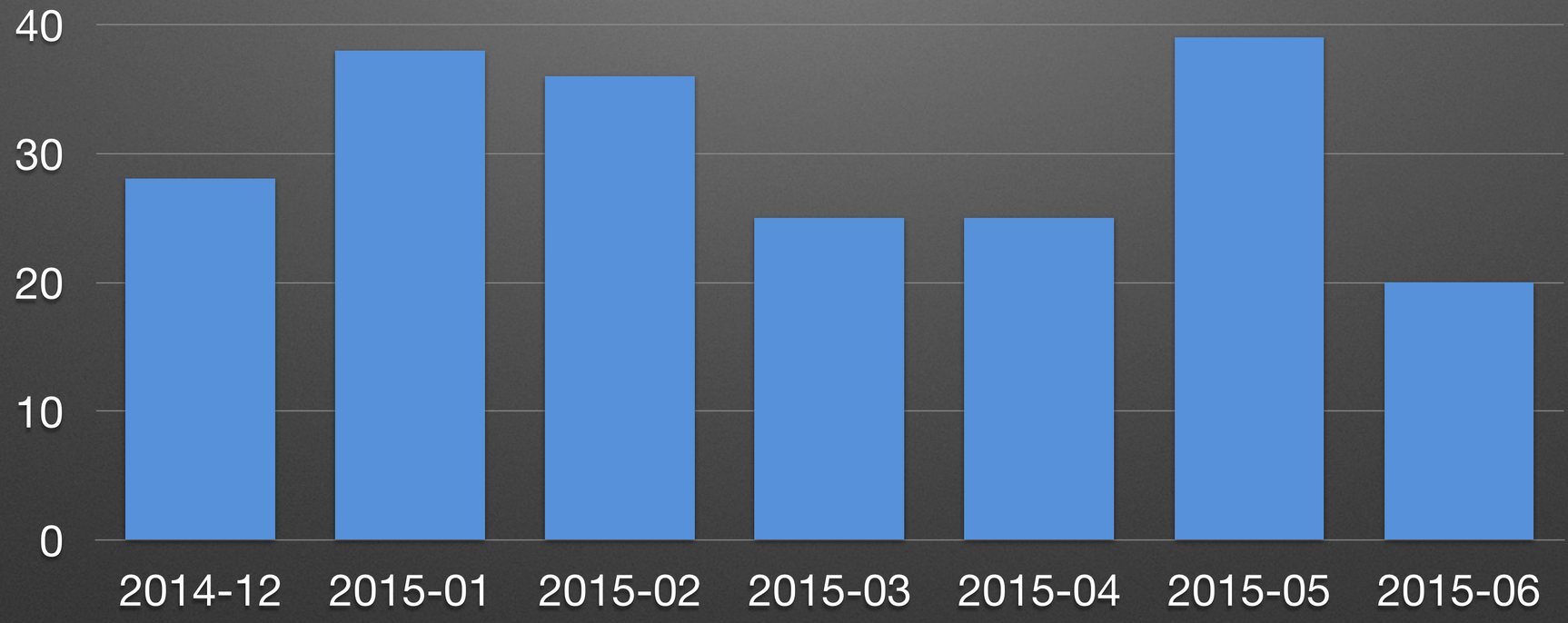
http://bit.ly/fastnetmon

FastNetMon

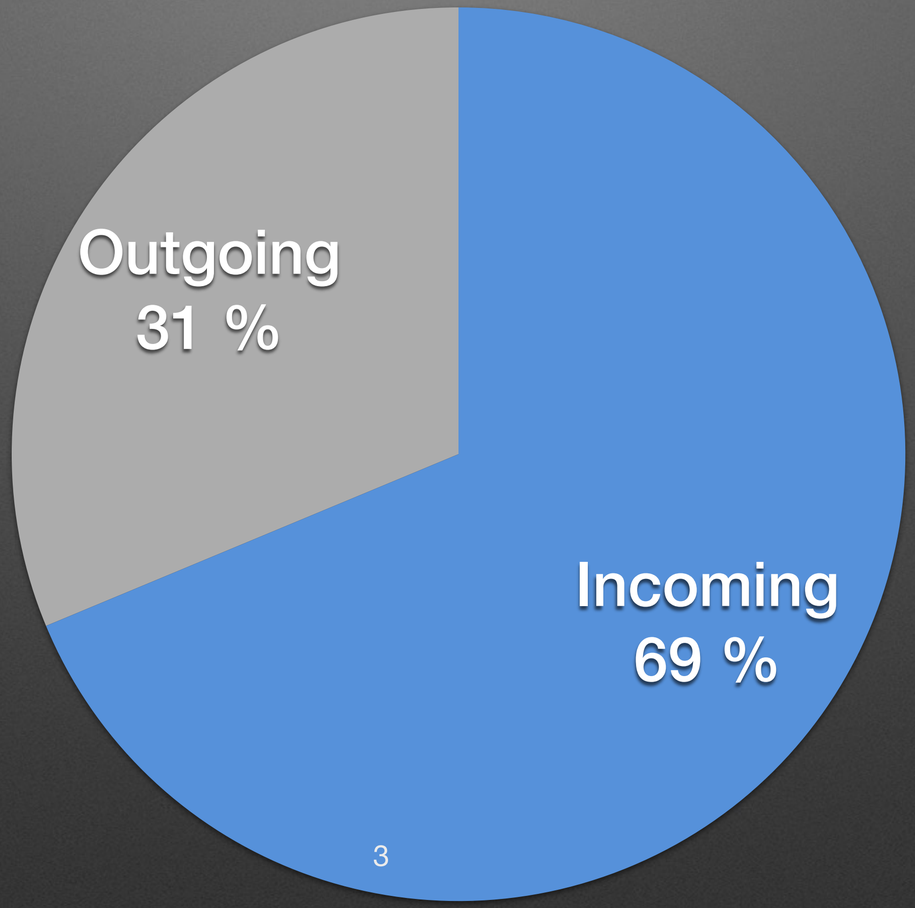
Open source DDoS mitigation toolkit

Pavel Odintsov
odintsov@fastvps.ee

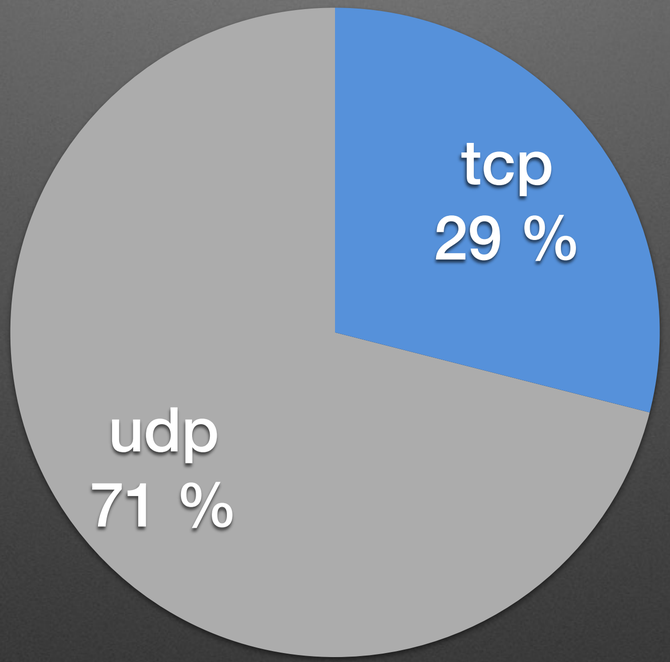
Number of DDoS attacks per month



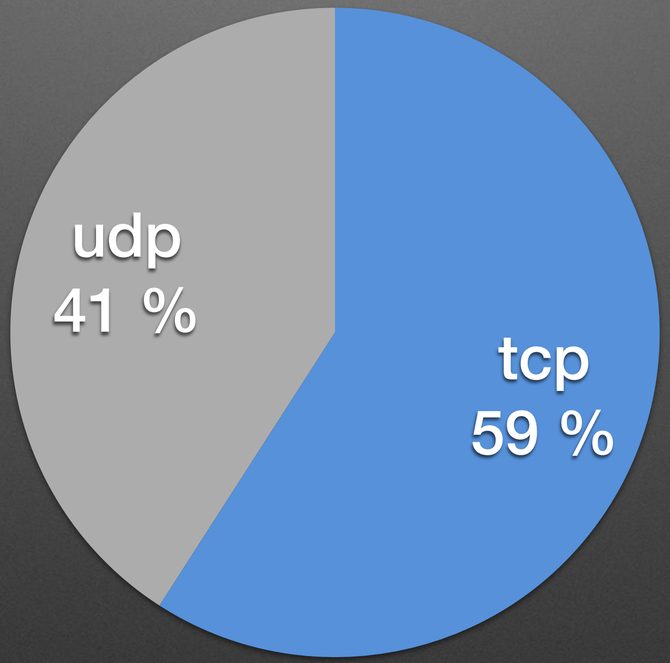
DDoS attack directions



Incoming DDoS attacks protocols

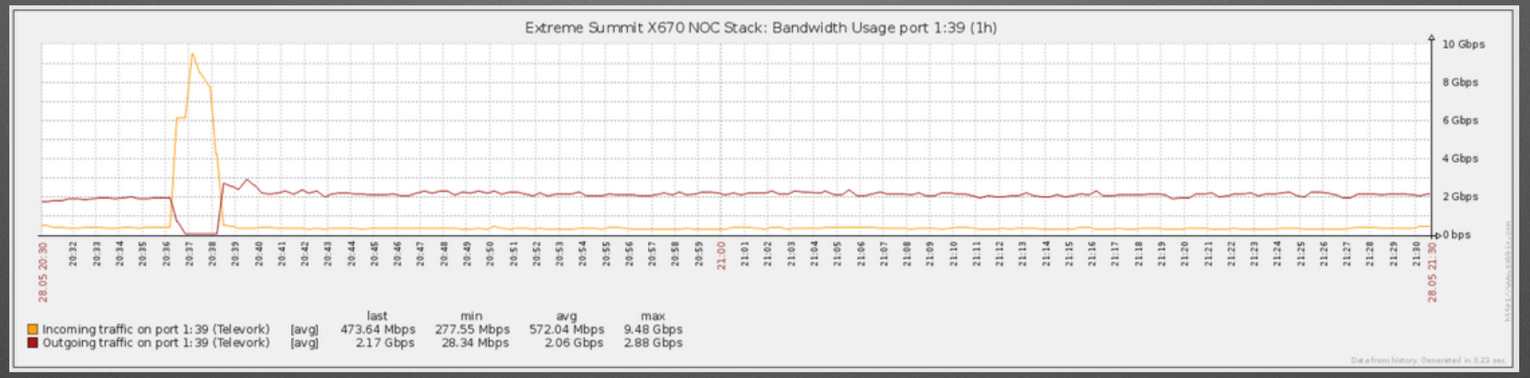


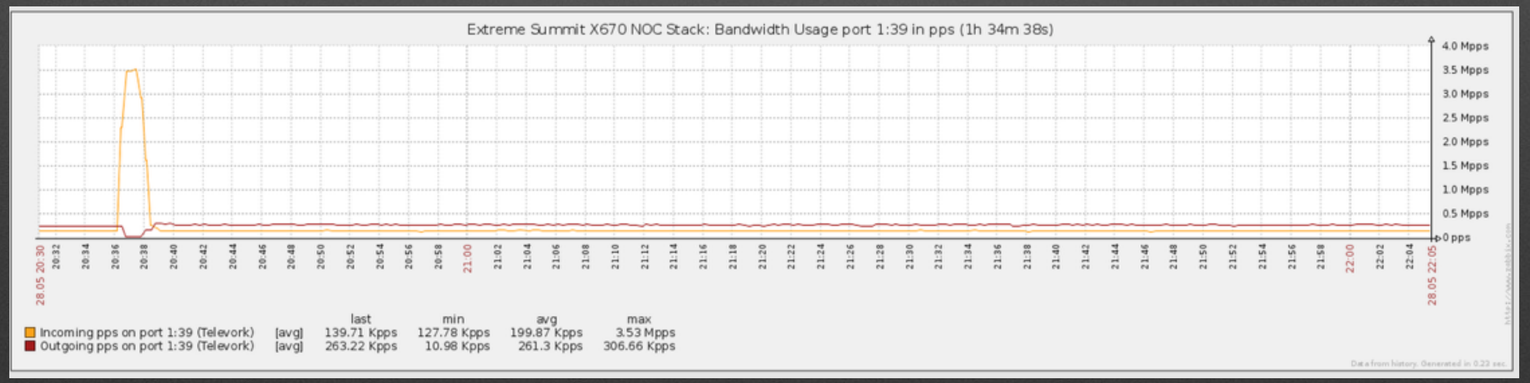
Outgoing DDoS attacks protocols



http://bit.ly/fastnetmon

Is it dangerous?





Any solutions?

FastNetMon

http://bit.ly/fastnetmon

What we could do?

- Save NOC’s sleep :)
- Detect any DoS/DDoS attack for channel overflow or equipment overload
- Partially or completely block traffic from/to own host (target of attack)
- Save your network (routers, switches, servers)
- Save your SLA

FastNetMon supported packet capture engines

- sFlow v5 (sampled traffic collection from switches)
- NetFlow v5, v9, v10 (sampled traffic data from routers)
- IPFIX (sampled traffic data from routers)
- Span/mirror (routers/switches deep inspection mode)

How we could block attack?

- BGP announce (community 666, blackhole, selective blackhole)
- BGP flow spec/RFC 5575 (selective traffic blocking)
- ACL on switch
- Custom script

Supported platforms

- Hyper-V, ESXi, KVM - we offer appliance based on VyOS
- CentOS/RHEL/Fedora Linux
- Debian/Ubuntu Linux
- FreeBSD

Hardware requirements

- 1 GE NIC (10GE recommended for mirror/span modem, Intel NIC's only)
- Intel Xeon CPU (E5 v3 recommended for high speed capture from mirror)
- 10GB hard disk drive

Performance

- sFLOW - 40-100GE
- NetFLOW - 40-100GE
- Span/mirror - 10-40GE per node (tested up to 10 MPPS)

Supported vendors

- Cisco
- Juniper
- Extreme
- Huawei
- Linux (ipt_NETFLOW)

Attack detection logic

- By number of packets per second to/from /32
- By number of mbps per second from/to /32
- By number of flows per second from/to /32
- By number of fragmented packets from/to /32
- By number of tcp syn packets from/to /32
- By number of udp packets from/to /32

Complete support for most popular attacks for channel overflow

- SYN flood
- UDP amplification (SSDP, Chargen, DNS, SNMP, NTP)
- IP fragmentation

Example attack report

IP: 10.10.10.221

Attack type: syn_flood

Initial attack power: 546475 packets per second

Peak attack power: 546475 packets per second

Attack direction: incoming

Attack protocol: tcp

Total incoming traffic: 245 mbps

Total outgoing traffic: 0 mbps

Total incoming pps: 99059 packets per second

Total outgoing pps: 0 packets per second

Total incoming flows: 98926 flows per second

Total outgoing flows: 0 flows per second

Average incoming traffic: 45 mbps

Average outgoing traffic: 0 mbps

Average incoming pps: 99059 packets per second

Average outgoing pps: 0 packets per second

Incoming ip fragmented traffic: 250 mbps

Outgoing ip fragmented traffic: 0 mbps

Incoming ip fragmented pps: 546475 packets per second

Outgoing ip fragmented pps: 0 packets per second

Incoming tcp traffic: 250 mbps

Outgoing tcp traffic: 0 mbps

Incoming tcp pps: 546475 packets per second

Outgoing tcp pps: 0 packets per second

Incoming syn tcp traffic: 250 mbps

Outgoing syn tcp traffic: 0 mbps

Incoming syn tcp pps: 546475 packets per second

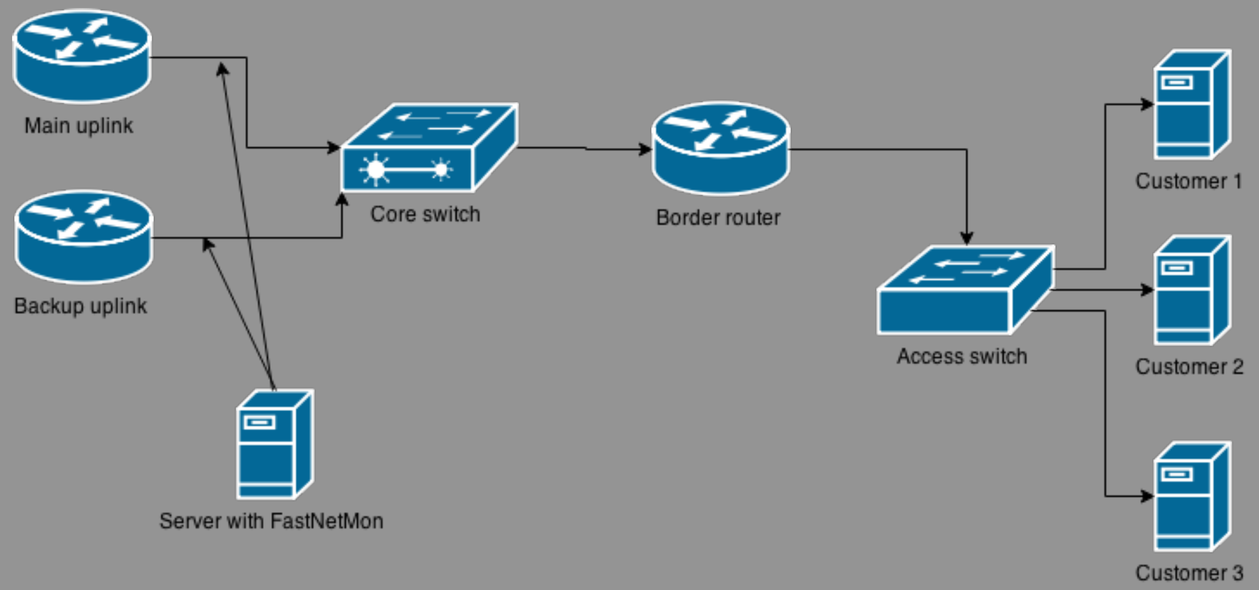
Outgoing syn tcp pps: 0 packets per second

Incoming udp traffic: 0 mbps

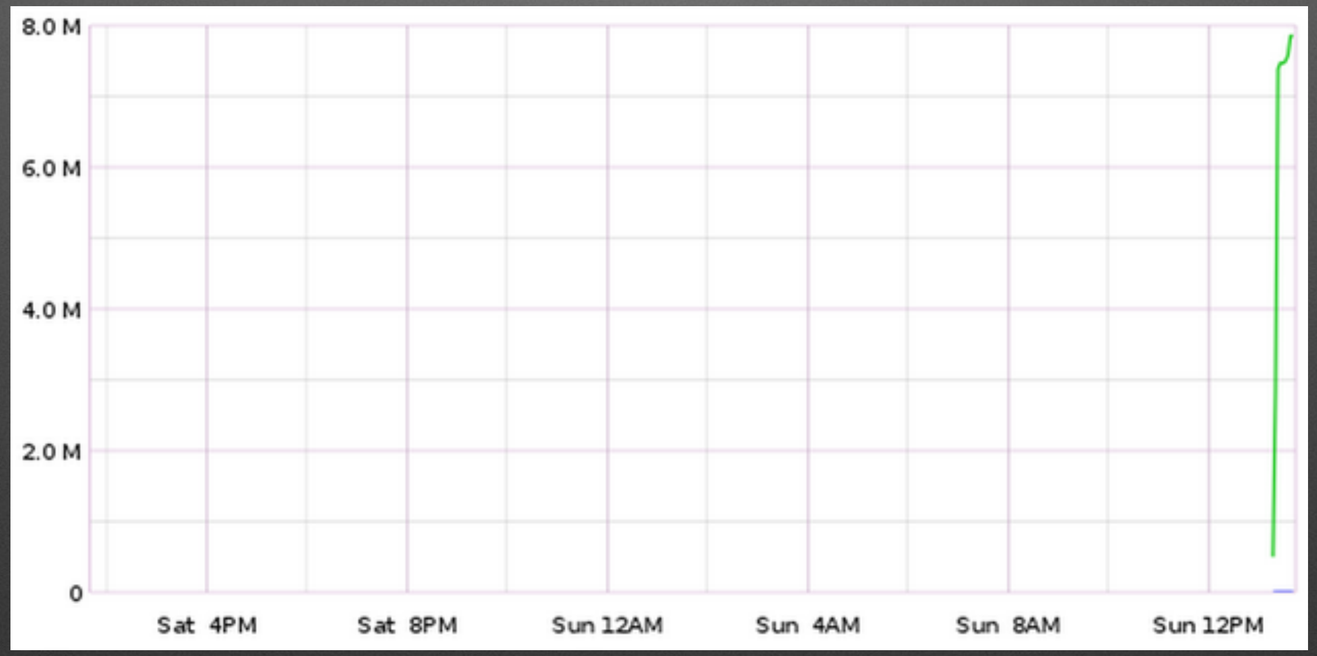
Outgoing udp traffic: 0 mbps

Incoming udp pps: 0 packets per second

Deploy scheme



Attack visualization in Graphite



How I can help?

- If you are Internet Carrier, please offer BGP blackhole for customers
- If you are Home ISP or Data Center, please filter outgoing attacks with big attention
- Contribute to FastNetMon on GitHub!
- Share knowledge about DDoS mitigation

http://bit.ly/fastnetmon

Thank you for attention!

pavel.odintsov@gmail.com