http://bit.ly/1QkyU2e

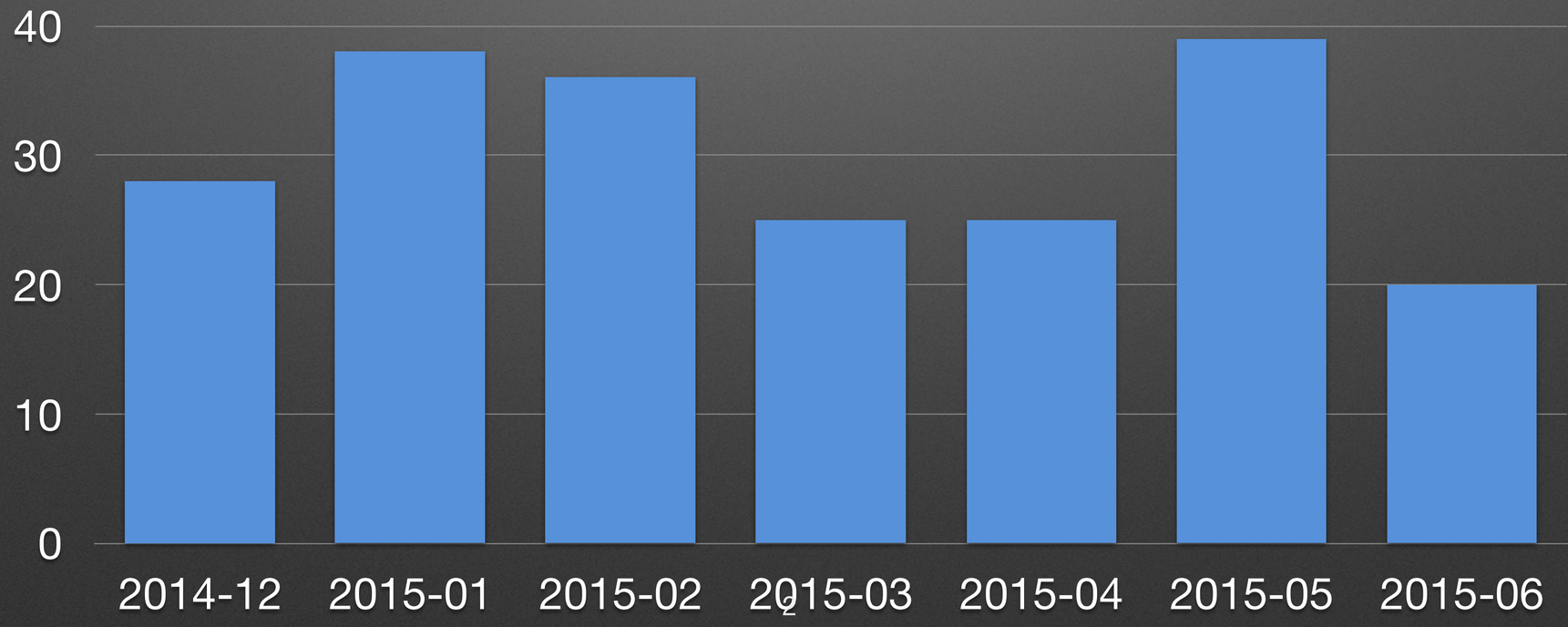
FastNetMon

Open source DDoS mitigation toolkit

Pavel Odintsov
odintsov@fastvps.ee

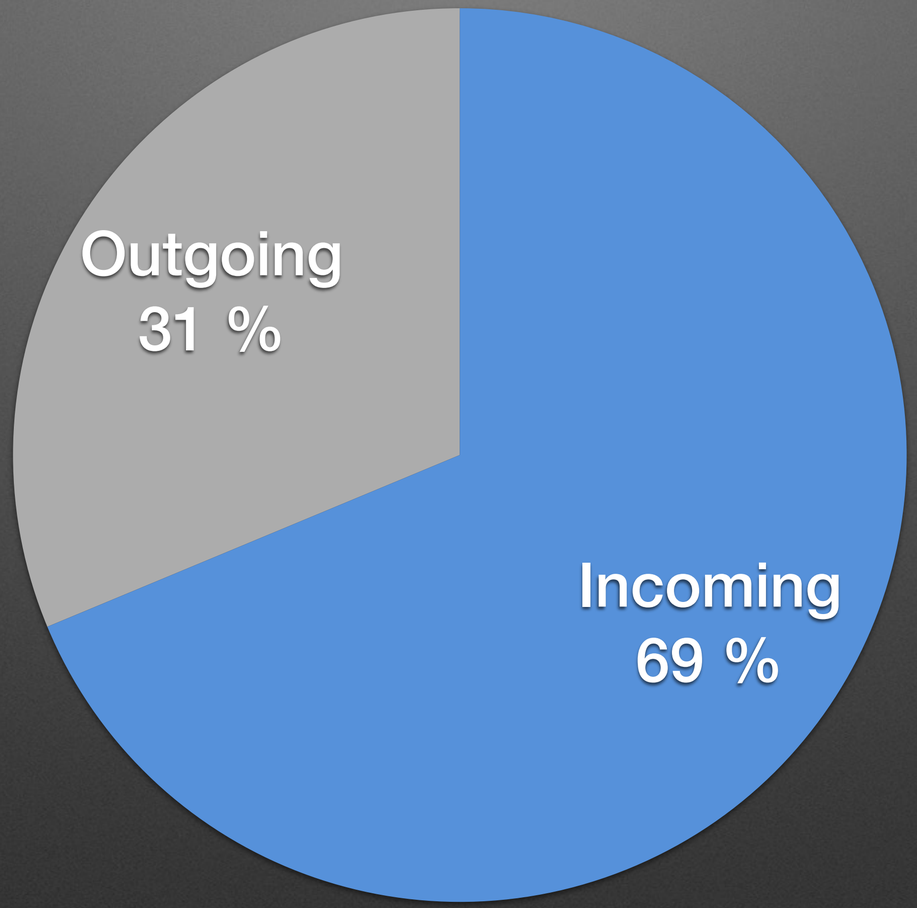
http://bit.ly/1QkyU2e

Number of DDoS attacks per month for VPS hosting provider



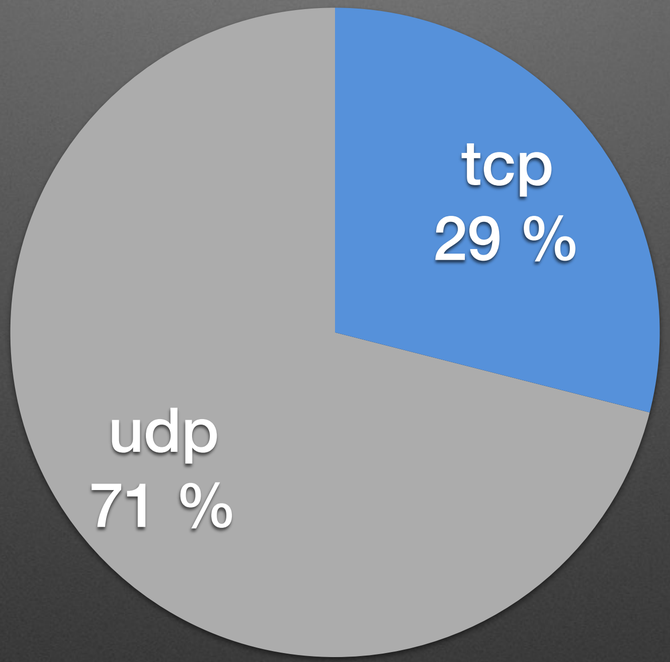
http://bit.ly/1QkyU2e

DDoS attack directions



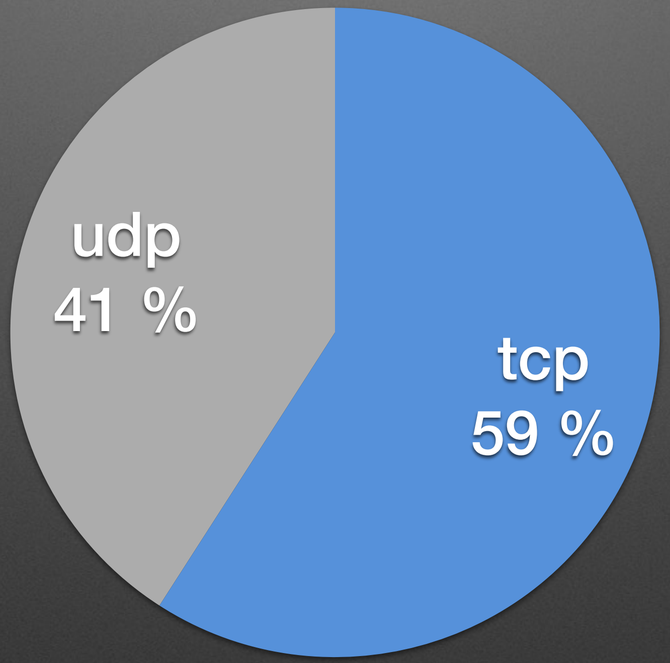
http://bit.ly/1QkyU2e

Incoming DDoS attacks protocols



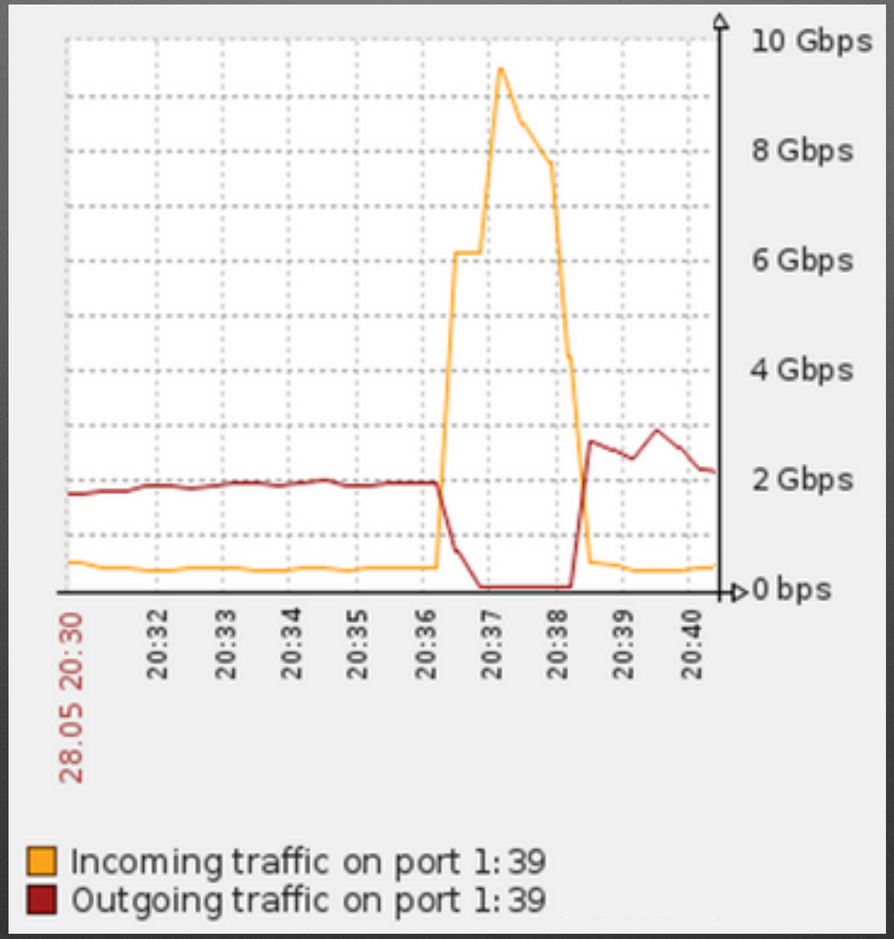
http://bit.ly/1QkyU2e

Outgoing DDoS attacks protocols



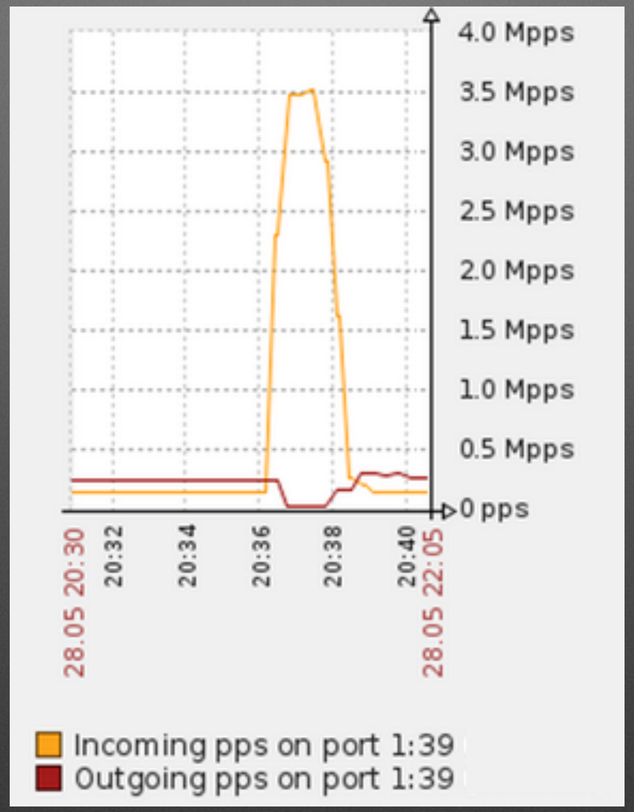
http://bit.ly/1QkyU2e

Is it dangerous — bandwidth?



http://bit.ly/1QkyU2e

Is it dangerous — pps?



http://bit.ly/1QkyU2e

Any solutions?

Hardware solutions

Cloud solutions

http://bit.ly/1QkyU2e

What wrong with they?

http://bit.ly/1QkyU2e

What wrong with current DDoS equipment?

- Too expensive!
- Need dedicated qualified network engineers
- Need significant changes in network architecture
- Not fully automated!
- Useless in case of channel overflow

http://bit.ly/1QkyU2e

What wrong with DDoS services?

- Increased latency
- Significant reaction time (BGP propagation time)
- Still need tool for trigger traffic diversion/redirection
- No outgoing attack mitigation
- Security reasons
- Single point of failure (SPoF)
- Very costly for «always on» mode
- Service could be broken by attack to another client

Silver bullet - FASTNETMON!

FastNetMon

http://bit.ly/1QkyU2e

http://bit.ly/1QkyU2e

What we could do?

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

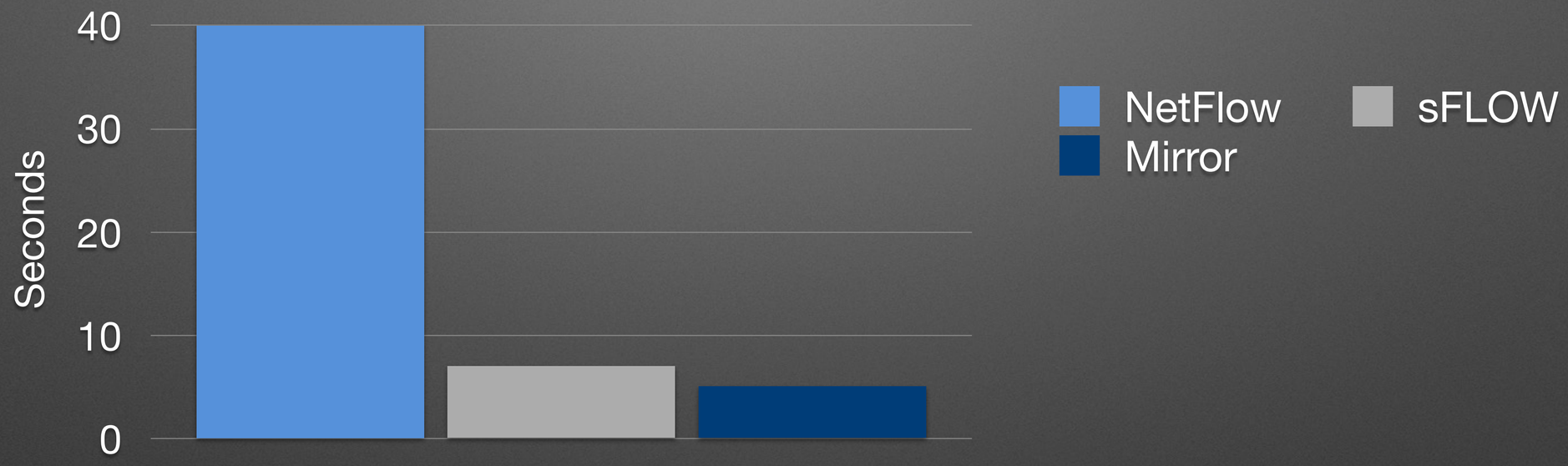
http://bit.ly/1QkyU2e

FastNetMon supported packet capture engines

- sFlow v4, 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)

http://bit.ly/1QkyU2e

Detection time for capture backends



http://bit.ly/1QkyU2e

Officially supported distributions

- CentOS 6
- CentOS 7
- Ubuntu 12.04
- Ubuntu 14.04
- Debian 6
- Debian 7
- Debian 8
- VyOS 1.1.6
- FreeBSD 9, 10, 11 (we are in official ports)

http://bit.ly/1QkyU2e

How we could block attack?

- BGP announce (community 666, blackhole, selective blackhole)
- BGP flow spec/RFC 5575 (selective traffic blocking: GoBGP, ExaBGP)
- Custom script
- Custom web callback script

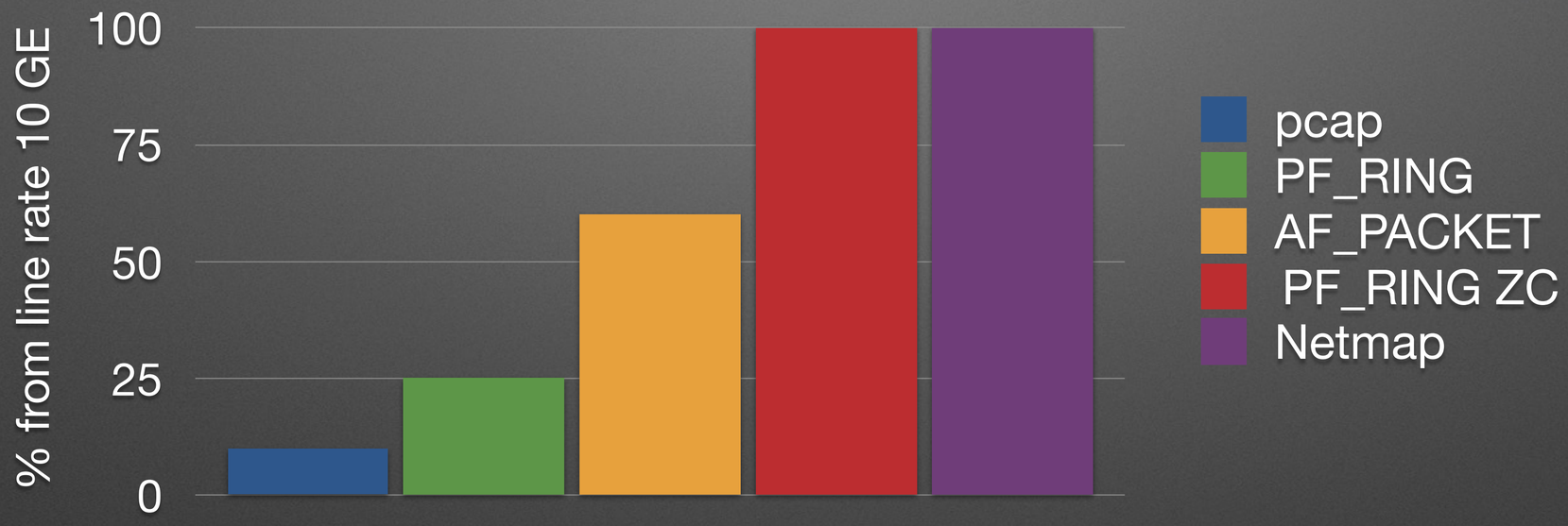
http://bit.ly/1QkyU2e

Supported vendors

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

http://bit.ly/1QkyU2e

Mirror capture performance



http://bit.ly/1QkyU2e

How to install on Linux?

wget https://raw.githubusercontent.com/FastVPSEestiOu/fastnetmon/master/src/fastnetmon_install.pl -Ofastnetmon_install.pl
sudo perl fastnetmon_install.pl --use-git-master

If you want «stable» 1.1.2 version please skip --use-git-master

http://bit.ly/1QkyU2e

Configuration

Main configuration file stored in /etc/fastnetmon.conf

Main log file stored in /var/log/fastnetmon.log

CLI client tool /opt/fastnetmon/fastnetmon_client

http://bit.ly/1QkyU2e

Configure networks list

Enumerate your networks in file /etc/networks_list in CIDR form:

10.10.12.0/24
8.8.8.0/24
192.168.77.0/24
4.8.4.8/32

We could work well only with ~/16 networks.

http://bit.ly/1QkyU2e

DDoS notify script

```
notify_script_path = /usr/local/bin/notify_about_attack.sh

#!/bin/bash
email_notify="root,please_fix_this_email@domain.ru"

if [ "$4" = "unban" ]; then
    # No details arrived to stdin here
    # Unban actions if used
    exit 0
fi

if [ "$4" = "ban" ]; then
    cat | mail -s "FastNetMon Guard: IP $1 blocked because $2 attack with power $3 pps" $email_notify;
   exit 0
fi

if [ "$4" == "attack_details" ]; then
    cat | mail -s "FastNetMon Guard: IP $1 blocked because $2 attack with power $3 pps" $email_notify;
    exit 0
fi
```

http://bit.ly/1QkyU2e

Attack detection configuration

```
# Enable ban actions
enable_ban = on

# Enable sFLOW plugin
sflow = on
# Enable NetFlow. Please set active and incative flow timeout to 30 seconds
netflow = on

# Calculate traffic speed over X seconds
average_calculation_time = 30

#  How long host should stay locked
ban_time = 1800

# Action thresholds
ban_for_pps = on
threshold_pps = 100000
ban_for_bandwidth = on
threshold_mbps = 1000
```

http://bit.ly/1QkyU2e

Starting up!

systemctl start fastnetmon
service fastnetmon start
/opt/fastnetmon/fastnetmon --daemonize

http://bit.ly/1QkyU2e

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

Outgoing udp pps: 0 packets per second

http://bit.ly/1QkyU2e

Core algorithms

- We count number of packets/bytes per protocol to/from /32 host with moving average
- We use moving average for average_calculation_time seconds for all counters.
- We count total number of bytes/packets for each monitored subnet

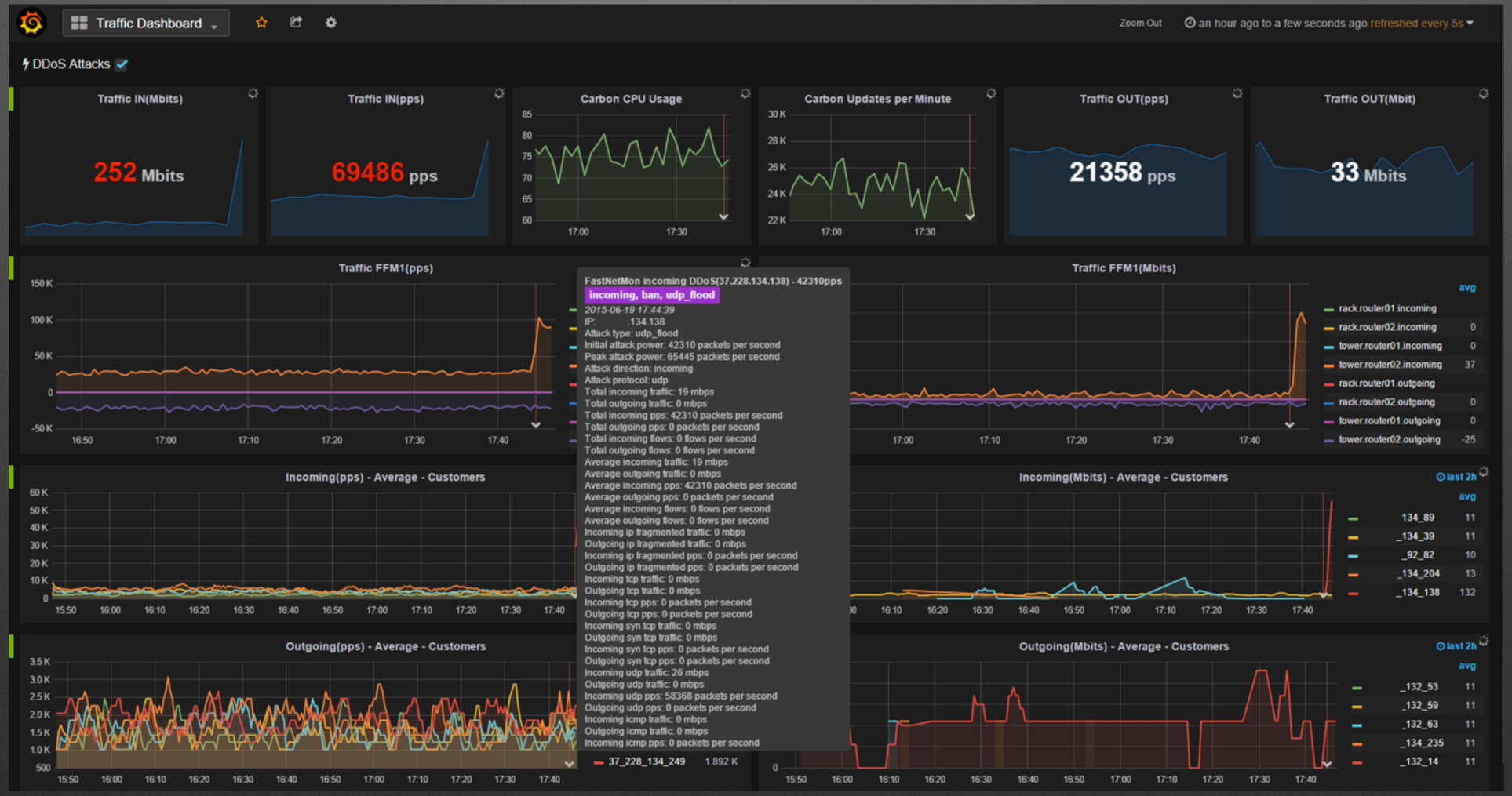
http://bit.ly/1QkyU2e

DPI

- 100% guarantee against false positive attack detection
- Supported only for mirror/SPAN because packet body required
- Used as second level for detection algorithm
- Very useful for networks
- Complete support for SNMP, DNS, NTP, SSDP amplification attacks

http://bit.ly/1QkyU2e

Attack visualization in Grafana



I need help!

- Mail list: https://groups.google.com/forum/#!forum/fastnetmon
- Bug tracker GitHub: http://bit.ly/1QkyU2e
- Twitter: https://twitter.com/odintsov_pavel
- IRC channel: #fastnetmon irc.freenode.net
- Author's email: pavel.odintsov@gmail.com (last resort!)

http://bit.ly/1QkyU2e

Thank you for attention!

pavel.odintsov@gmail.com

http://bit.ly/1QkyU2e

Bonus slides!

http://bit.ly/1QkyU2e

Traffic capture subsystem

- sFLOW v4, v5
- NetFlow v5, v9, v10 (IPFIX)
- Port mirroring, SPAN, RSPAN

http://bit.ly/1QkyU2e

sFLOW

- FastNetMon: sflow = on
- Supported by almost any switch
- No aggregation (detailed per host and per port data)
- No flow lag (fast attack detection without lag)
- Enough accurate traffic bandwidth
- Be careful with sampling! 10GE - 1024-2048.
- Has packet header for analytics
- Could be filtered with LUA script (complex deployments with multiple traffic paths)

http://bit.ly/1QkyU2e

Netflow

- FastNetMon: netflow = on
- Could be sampled (be careful with sampling rate or do not use it), configured manually with netflow_sampling_ratio.
- Has significant (~30 seconds) flow lag (+lag time to attack detection time)
- Please setup flow active timeout and flow inactive timeout to smallest possible value!
- Could kill your control plane CPU (software implementation)
- Could overload service link for NetFlow data
- Not so accurate bandwidth data
- Please set average_calculation_time to max(flow_active, flow_inactive)
- Haven’t any packet header information
- Could be filtered with LUA script (MPLS, complex deployments)

http://bit.ly/1QkyU2e

Mirror traffic capture

- pcap
- PF_RING
- Netmap
- AF_PACKET
- SnabbSwitch

http://bit.ly/1QkyU2e

pcap

- FastNetMon: pcap = on
- Work everywhere
- Very slow, really it will die on 200-300 000 packets per second

http://bit.ly/1QkyU2e

Netmap

- FastNetMon: mirror_netmap = on
- Bundled support in FreeBSD kernel
- Open source Linux kernel module
- Line rate for 10GE on old hardware
- Need patched driver on Linux (only Intel supported)
- Really fast attack detection
- Has whole packet data (DPI could be used)
- Could be used on sampled mirror (netmap_sampling_ratio)
- Could be used on cropped mirror (Juniper: maximum-packet-length, use option netmap_read_packet_length_from_ip_header)
- Could collect pcap attack fingerprint

http://bit.ly/1QkyU2e

PF_RING

- FastNetMon: mirror = on
- Only Linux
- Only Intel NIC + additional license for line rate capture (enable_pf_ring_zc_mode)
- Need patched driver on Linux for line rate capture
- Really fast attack detection
- Has whole packet data (DPI could be used)
- Could be used on sampled mirror (pfring_sampling_ratio)
- Could collect pcap attack fingerprint

http://bit.ly/1QkyU2e

AF_PACKET

- mirror_afpacket = on
- Buggy before Linux 3.6
- Bundled in Linux kernel
- Could do 80% of line rate on 10GE (~9 Mpps)
- Work anywhere (PowerPC, ARM, …)
- Fast attack detection and no external dependencies

http://bit.ly/1QkyU2e

SnabbSwitch

- mirror_snabbswitch = on
- Lua powered 82599 NIC driver
- Very fast!
- Very flexible!
- Really fun!
- You should specify interfaces with PCI addresses:
  interfaces_snabbswitch = 0000:04:00.0,0000:04:00.1