FastNetMon

Omid Kosari

Current DDOS protection main problems

- Price
- Sanctions
- Hard to implement
- Not useful for small/medium size companies
- Needs special learnings

What we achieve ?

- Better NOC Sleep
- Less complain from customers
- Less bandwidth waste

Real world DDOS examples

- **Many** G/T bit attack to **few** hosts under your network
  - Simple detection
- **Few** Gbit attack to **many** hosts under your network
  - Very complex detection
  - Needs automated mitigation

Key Features

- Ability to detect and filter out only malicious traffic flowing into or from your network.
- Flexible detection engine with support for DoS/DDoS attack types: amplification (NTP, SNMP, SSDP, DNS, GRE, chargen and other), floods (UDP, TCP, ICMP), attacks on tcp protocol (syn, syn-ack, fin floods), attacks on IP protocol (fragmented packets) and other. Including support for multi-vector attacks.
- Very fast detection time: 1 second for sFlow 5 and port mirror mode and 5- 45 seconds for Netflow/IPFIX (depends in device model).
- Scalable up to Terabits (multiple existing deployments with 1+ Tbps of traffic).
- **Lua friendly**

Deployment Features

- Wide range of supported capture engines: sFlow v5, Netflow v5, v9, jFlow, IPFIX (including complete support for sampled flows), mirror ports (sampled).
- Bundled BGP and BGP flow spec (RFC 5575) support.
- Could use existing devices in your network for traffic filtration/blocking
- Bundled support industry-leading tool for querying and visualizing traffic information: Grafana.
- Very fast delivery time: about 40 minutes for installation and initial configuration (excludes network equipment configuration and time required for server preparation).

Deployment Features

- Tested compatibility with following vendors: Cisco, Juniper, Alcatel, Huawei, Mikrotik, Extreme, Arista, Brocade, Dell, HP, Palo Alto, D-Link, Edge Core, Ericsson, Force and other.
- Software based solution, you do not need any specific hardware, you could use any VM or server available on your local market.
- Network engineers friendly command line configuration tool: fcli.
- Developers friendly: API, hook scripts, filter scripts. JSON based database for configuration/attacks with wide range of client tools for different languages.

Supported Platforms

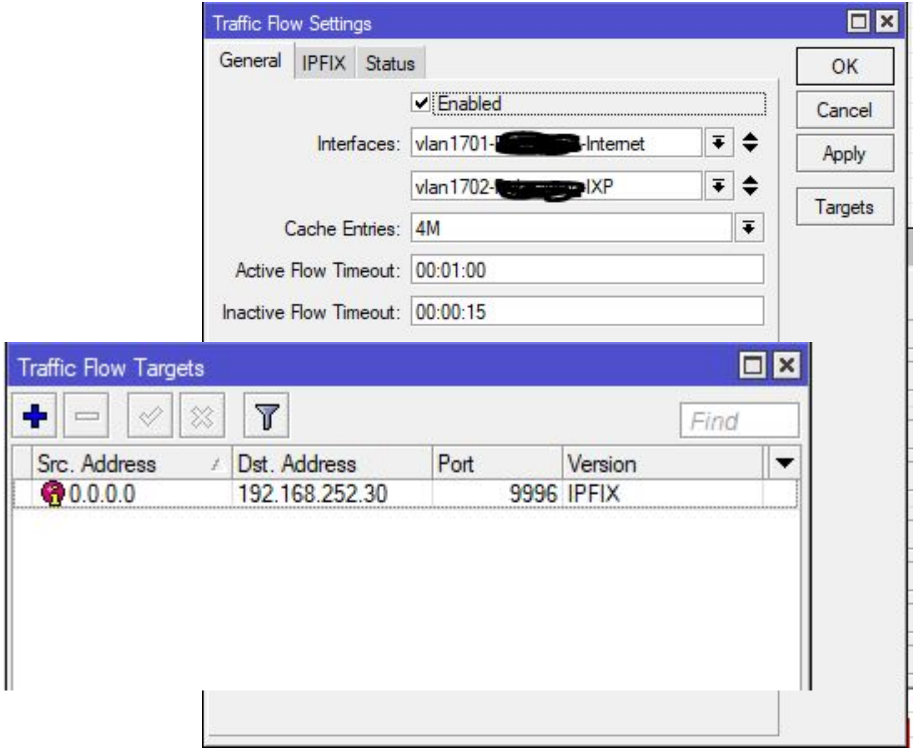
- Linux (Debian 6/7/8/9, CentOS 6/7, Ubuntu 12.04, 14.04, 16.04)
- FreeBSD 9, 10, 11: official port.
- Mac OS X Yosemite (only 1.1.2 release)

Let’s dirty your hands

```
#wget https://raw.githubusercontent.com/pavel-odintsov/fastnetmon/master/src/fastnetmon_install.pl -Ofastnetmon_install.pl

#sudo perl fastnetmon_install.pl

#nano /etc/networks_list

#nano /etc/networks_whitelist
```

Simple way - Netflow

IP > Traffic Flow



☑ Enabled

Interfaces: vlan1701-[redacted]-Internet

vlan1702-[redacted]IXP

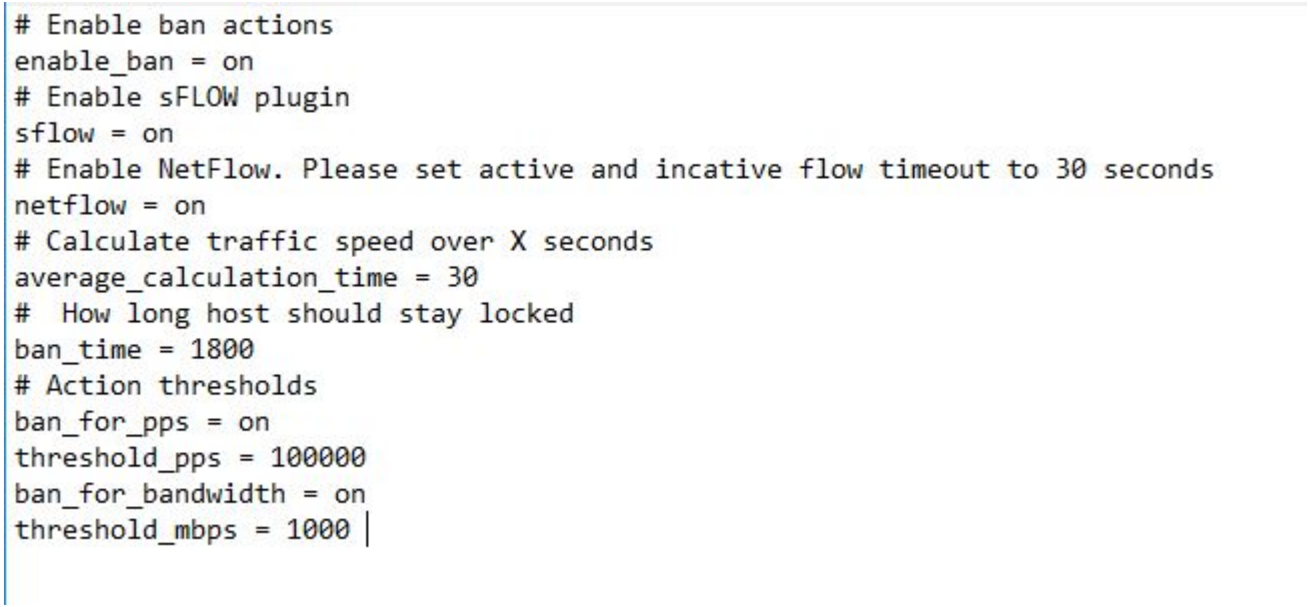
Cache Entries: 4M

Active Flow Timeout: 00:01:00

Inactive Flow Timeout: 00:00:15

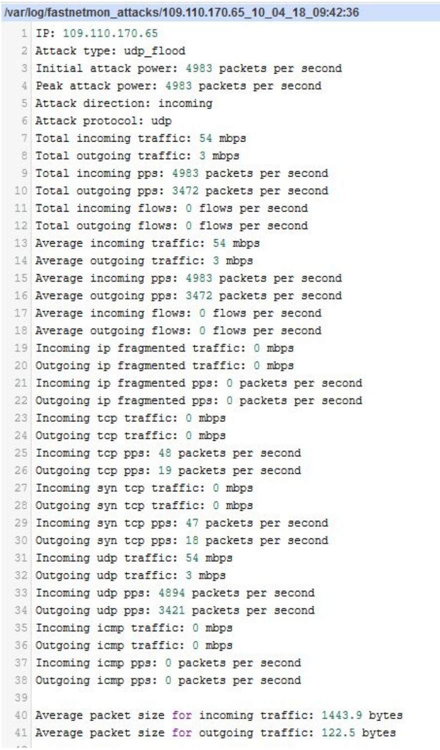
Src. Address	Dst. Address	Port	Version
0.0.0.0	192.168.252.30	9996	IPFIX

/etc/fastnetmon.conf



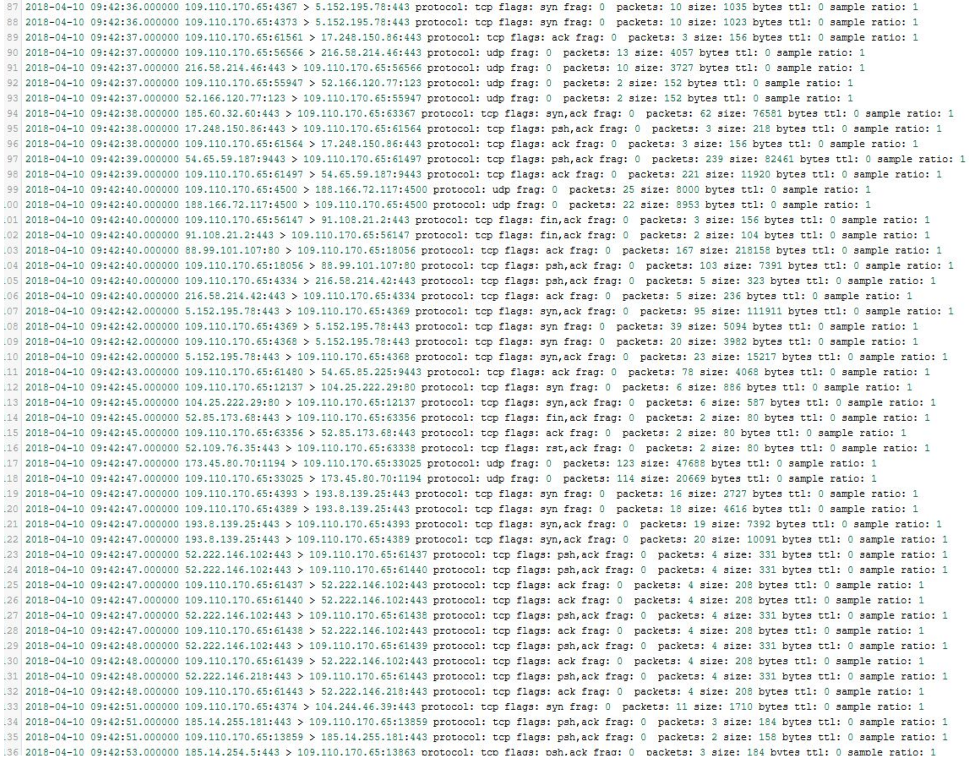
```
# Enable ban actions
enable_ban = on
# Enable sFLOW plugin
sflow = on
# Enable NetFlow. Please set active and incative flow timeout to 30 seconds
netflow = on
# Calculate traffic speed over X seconds
average_calculation_time = 30
#  How long host should stay locked
ban_time = 1800
# Action thresholds
ban_for_pps = on
threshold_pps = 100000
ban_for_bandwidth = on
threshold_mbps = 1000
```

```
#/opt/fastnetmon/fastnetmon --daemonize
```



/var/log/fastnetmon_attacks/109.110.170.65_10_04_18_09:42:36

```
IP: 109.110.170.65
Attack type: udp_flood
Initial attack power: 4983 packets per second
Peak attack power: 4983 packets per second
Attack direction: incoming
Attack protocol: udp
Total incoming traffic: 54 mbps
Total outgoing traffic: 3 mbps
Total incoming pps: 4983 packets per second
Total outgoing pps: 3472 packets per second
Total incoming flows: 0 flows per second
Total outgoing flows: 0 flows per second
Average incoming traffic: 54 mbps
Average outgoing traffic: 3 mbps
Average incoming pps: 4983 packets per second
Average outgoing pps: 3472 packets per second
Average incoming flows: 0 flows per second
Average outgoing flows: 0 flows per second
Incoming ip fragmented traffic: 0 mbps
Outgoing ip fragmented traffic: 0 mbps
Incoming ip fragmented pps: 0 packets per second
Outgoing ip fragmented pps: 0 packets per second
Incoming tcp traffic: 0 mbps
Outgoing tcp traffic: 0 mbps
Incoming tcp pps: 48 packets per second
Outgoing tcp pps: 19 packets per second
Incoming syn tcp traffic: 0 mbps
Outgoing syn tcp traffic: 0 mbps
Incoming syn tcp pps: 47 packets per second
Outgoing syn tcp pps: 18 packets per second
Incoming udp traffic: 54 mbps
Outgoing udp traffic: 3 mbps
Incoming udp pps: 4894 packets per second
Outgoing udp pps: 3421 packets per second
Incoming icmp traffic: 0 mbps
Outgoing icmp traffic: 0 mbps
Incoming icmp pps: 0 packets per second
Outgoing icmp pps: 0 packets per second

Average packet size for incoming traffic: 1443.9 bytes
Average packet size for outgoing traffic: 122.5 bytes
```

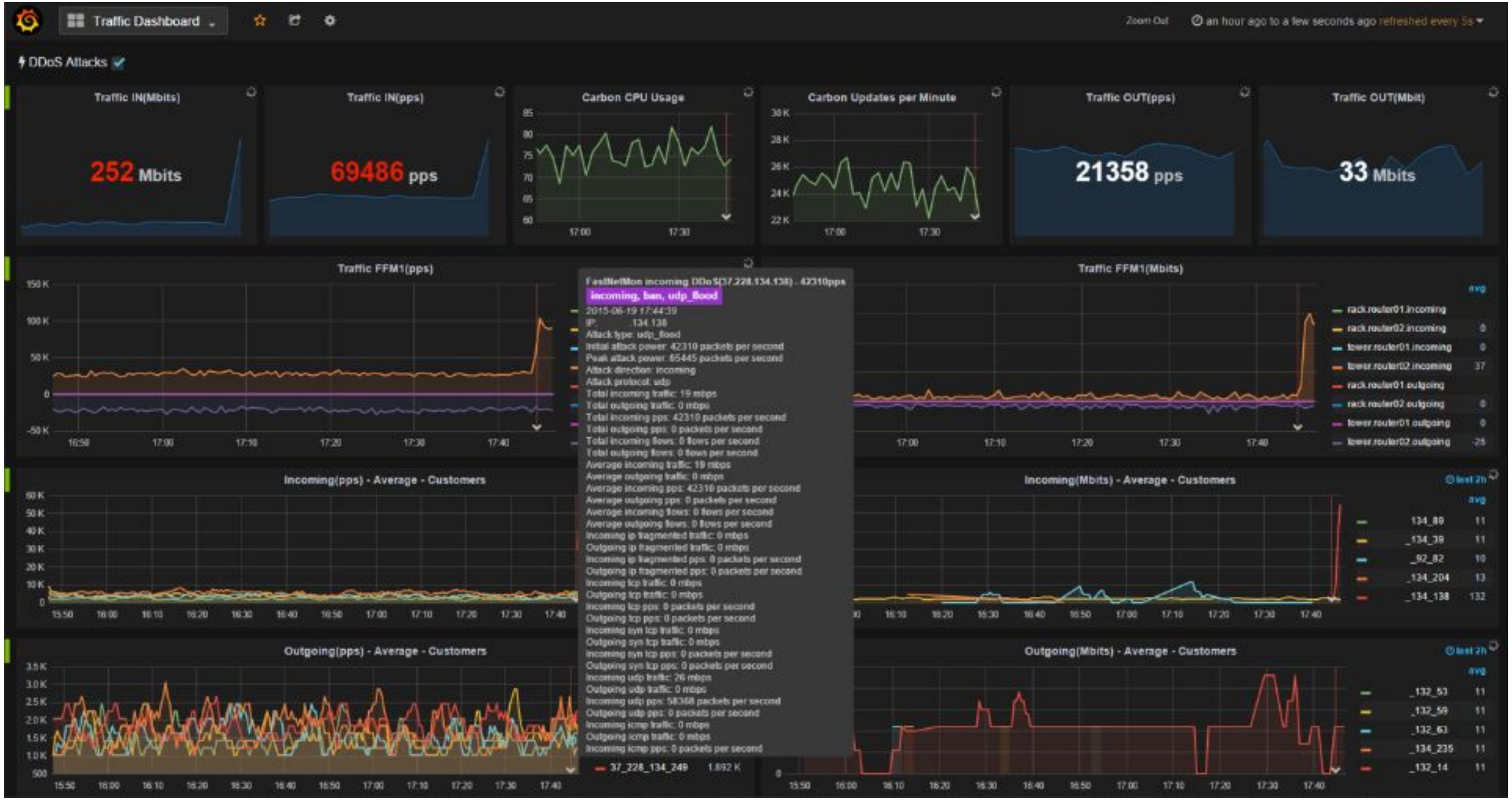


```
2018-04-10 09:42:36.000000 109.110.170.65:4367 > 5.152.195.78:443 protocol: tcp flags: syn frag: 0  packets: 10 size: 1035 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:36.000000 109.110.170.65:4373 > 5.152.195.78:443 protocol: tcp flags: syn frag: 0  packets: 10 size: 1023 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:37.000000 109.110.170.65:61561 > 17.248.150.86:443 protocol: tcp flags: ack frag: 0  packets: 3 size: 156 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:37.000000 109.110.170.65:56566 > 216.58.214.46:443 protocol: udp frag: 0  packets: 13 size: 4057 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:37.000000 216.58.214.46:443 > 109.110.170.65:56566 protocol: udp frag: 0  packets: 10 size: 3727 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:37.000000 109.110.170.65:55947 > 52.166.120.77:123 protocol: udp frag: 0  packets: 2 size: 152 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:37.000000 52.166.120.77:123 > 109.110.170.65:55947 protocol: udp frag: 0  packets: 2 size: 152 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:38.000000 185.60.32.60:443 > 109.110.170.65:63367 protocol: tcp flags: syn,ack frag: 0  packets: 62 size: 76581 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:38.000000 17.248.150.86:443 > 109.110.170.65:61564 protocol: tcp flags: psh,ack frag: 0  packets: 3 size: 218 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:38.000000 109.110.170.65:61564 > 17.248.150.86:443 protocol: tcp flags: ack frag: 0  packets: 3 size: 156 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:39.000000 54.65.59.187:9443 > 109.110.170.65:61497 protocol: tcp flags: psh,ack frag: 0  packets: 239 size: 82461 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:39.000000 109.110.170.65:61497 > 54.65.59.187:9443 protocol: tcp flags: ack frag: 0  packets: 221 size: 11920 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 109.110.170.65:4500 > 188.166.72.117:4500 protocol: udp frag: 0  packets: 25 size: 8000 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 188.166.72.117:4500 > 109.110.170.65:4500 protocol: udp frag: 0  packets: 22 size: 8953 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 109.110.170.65:56147 > 91.108.21.2:443 protocol: tcp flags: fin,ack frag: 0  packets: 3 size: 156 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 91.108.21.2:443 > 109.110.170.65:56147 protocol: tcp flags: fin,ack frag: 0  packets: 2 size: 104 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 88.99.101.107:80 > 109.110.170.65:18056 protocol: tcp flags: ack frag: 0  packets: 167 size: 218158 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 109.110.170.65:18056 > 88.99.101.107:80 protocol: tcp flags: psh,ack frag: 0  packets: 103 size: 7391 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 109.110.170.65:4334 > 216.58.214.42:443 protocol: tcp flags: psh,ack frag: 0  packets: 5 size: 323 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:40.000000 216.58.214.42:443 > 109.110.170.65:4334 protocol: tcp flags: ack frag: 0  packets: 5 size: 236 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:42.000000 5.152.195.78:443 > 109.110.170.65:4369 protocol: tcp flags: syn,ack frag: 0  packets: 95 size: 111911 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:42.000000 109.110.170.65:4369 > 5.152.195.78:443 protocol: tcp flags: syn frag: 0  packets: 39 size: 5094 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:42.000000 109.110.170.65:4368 > 5.152.195.78:443 protocol: tcp flags: syn frag: 0  packets: 20 size: 3982 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:42.000000 5.152.195.78:443 > 109.110.170.65:4368 protocol: tcp flags: syn,ack frag: 0  packets: 23 size: 15217 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:43.000000 109.110.170.65:61480 > 54.65.85.225:9443 protocol: tcp flags: ack frag: 0  packets: 78 size: 4068 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:45.000000 109.110.170.65:12137 > 104.25.222.29:80 protocol: tcp flags: syn frag: 0  packets: 6 size: 886 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:45.000000 104.25.222.29:80 > 109.110.170.65:12137 protocol: tcp flags: syn,ack frag: 0  packets: 6 size: 587 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:45.000000 52.85.173.68:443 > 109.110.170.65:63356 protocol: tcp flags: fin,ack frag: 0  packets: 2 size: 80 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:45.000000 109.110.170.65:63356 > 52.85.173.68:443 protocol: tcp flags: ack frag: 0  packets: 2 size: 80 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 52.109.76.35:443 > 109.110.170.65:63338 protocol: tcp flags: rst,ack frag: 0  packets: 2 size: 80 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 173.45.80.70:1194 > 109.110.170.65:33025 protocol: udp frag: 0  packets: 123 size: 47688 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 109.110.170.65:33025 > 173.45.80.70:1194 protocol: udp frag: 0  packets: 114 size: 20669 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 109.110.170.65:4393 > 193.8.139.25:443 protocol: tcp flags: syn frag: 0  packets: 16 size: 2727 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 109.110.170.65:4389 > 193.8.139.25:443 protocol: tcp flags: syn frag: 0  packets: 18 size: 4616 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 193.8.139.25:443 > 109.110.170.65:4393 protocol: tcp flags: syn,ack frag: 0  packets: 19 size: 7392 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 193.8.139.25:443 > 109.110.170.65:4389 protocol: tcp flags: syn,ack frag: 0  packets: 20 size: 10091 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 52.222.146.102:443 > 109.110.170.65:61437 protocol: tcp flags: psh,ack frag: 0  packets: 4 size: 331 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 52.222.146.102:443 > 109.110.170.65:61440 protocol: tcp flags: psh,ack frag: 0  packets: 4 size: 331 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 109.110.170.65:61437 > 52.222.146.102:443 protocol: tcp flags: ack frag: 0  packets: 4 size: 208 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 109.110.170.65:61440 > 52.222.146.102:443 protocol: tcp flags: ack frag: 0  packets: 4 size: 208 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 52.222.146.102:443 > 109.110.170.65:61438 protocol: tcp flags: psh,ack frag: 0  packets: 4 size: 331 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:47.000000 109.110.170.65:61438 > 52.222.146.102:443 protocol: tcp flags: ack frag: 0  packets: 4 size: 208 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:48.000000 52.222.146.102:443 > 109.110.170.65:61439 protocol: tcp flags: psh,ack frag: 0  packets: 4 size: 331 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:48.000000 109.110.170.65:61439 > 52.222.146.102:443 protocol: tcp flags: ack frag: 0  packets: 4 size: 208 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:48.000000 52.222.146.218:443 > 109.110.170.65:61443 protocol: tcp flags: psh,ack frag: 0  packets: 4 size: 331 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:48.000000 109.110.170.65:61443 > 52.222.146.218:443 protocol: tcp flags: ack frag: 0  packets: 4 size: 208 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:51.000000 109.110.170.65:4374 > 104.244.46.39:443 protocol: tcp flags: syn frag: 0  packets: 11 size: 1710 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:51.000000 185.14.255.181:443 > 109.110.170.65:13859 protocol: tcp flags: psh,ack frag: 0  packets: 3 size: 184 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:51.000000 109.110.170.65:13859 > 185.14.255.181:443 protocol: tcp flags: psh,ack frag: 0  packets: 2 size: 158 bytes ttl: 0 sample ratio: 1
2018-04-10 09:42:53.000000 185.14.254.5:443 > 109.110.170.65:13863 protocol: tcp flags: psh,ack frag: 0  packets: 3 size: 184 bytes ttl: 0 sample ratio: 1
```

DPI

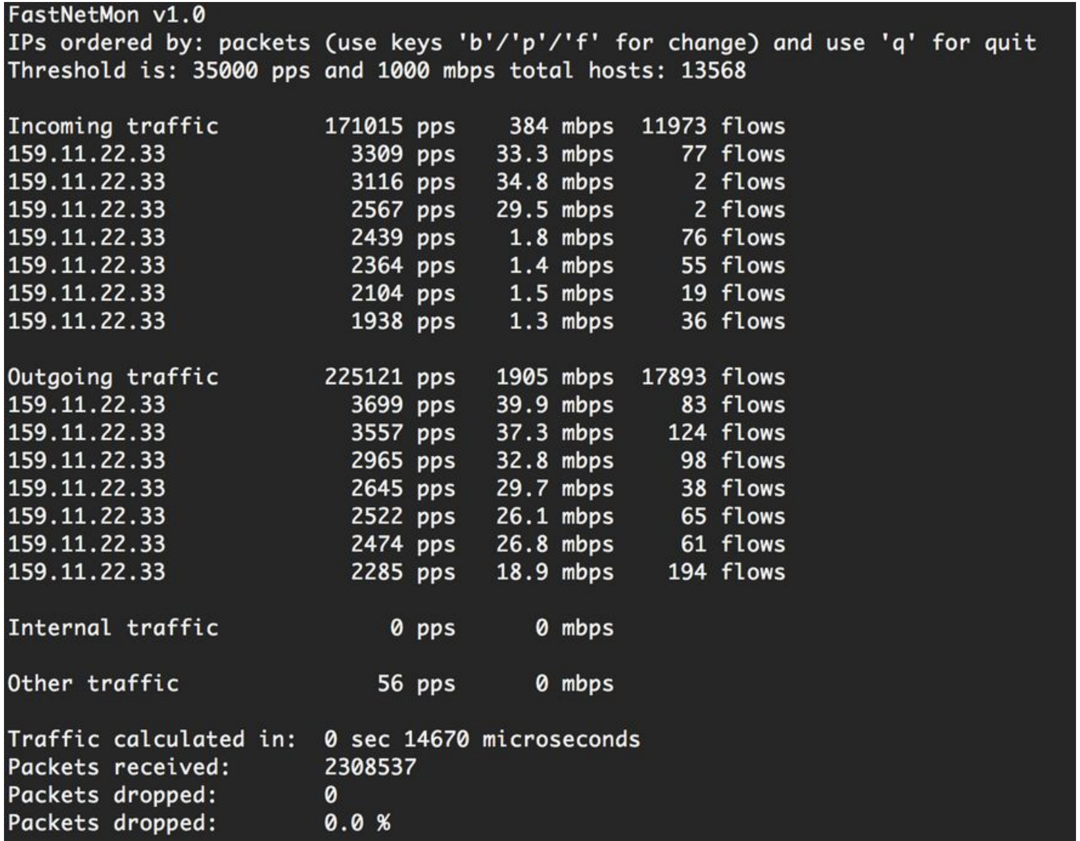
- 100% guarantee against false positive attack detection
- Supported only for mirror/SPAN because packet body required
- Used as second level for detection algorithm
- Very useful for networks
- Complete support for SNMP, DNS, NTP, SSDP amplification attacks

Attack visualization in Grafana



FastNetMon incoming DDoS(37.228.134.138) - 42310pps
incoming, ban, udp_flood
2015-06-19 17:44:39
IP: .134.138
Attack type: udp_flood
Initial attack power: 42310 packets per second
Peak attack power: 65445 packets per second
Attack direction: incoming
Attack protocol: udp
Total incoming traffic: 19 mbps
Total outgoing traffic: 0 mbps
Total incoming pps: 42310 packets per second
Total outgoing pps: 0 packets per second
Total incoming flows: 0 flows per second
Total outgoing flows: 0 flows per second
Average incoming traffic: 19 mbps
Average outgoing traffic: 0 mbps
Average incoming pps: 42310 packets per second
Average outgoing pps: 0 packets per second
Average incoming flows: 0 flows per second
Average outgoing flows: 0 flows per second
Incoming ip fragmented traffic: 0 mbps
Outgoing ip fragmented traffic: 0 mbps
Incoming ip fragmented pps: 0 packets per second
Outgoing ip fragmented pps: 0 packets per second
Incoming tcp traffic: 0 mbps
Outgoing tcp traffic: 0 mbps
Incoming tcp pps: 0 packets per second
Outgoing tcp pps: 0 packets per second
Incoming syn tcp traffic: 0 mbps
Outgoing syn tcp traffic: 0 mbps
Incoming syn tcp pps: 0 packets per second
Outgoing syn tcp pps: 0 packets per second
Incoming udp traffic: 26 mbps
Outgoing udp traffic: 0 mbps
Incoming udp pps: 58368 packets per second
Outgoing udp pps: 0 packets per second
Incoming icmp traffic: 0 mbps
Outgoing icmp traffic: 0 mbps
Incoming icmp pps: 0 packets per second

/opt/fastnetmon/fastnetmon_client



```
FastNetMon v1.0
IPs ordered by: packets (use keys 'b'/'p'/'f' for change) and use 'q' for quit
Threshold is: 35000 pps and 1000 mbps total hosts: 13568

Incoming traffic        171015 pps    384 mbps  11973 flows
159.11.22.33              3309 pps   33.3 mbps     77 flows
159.11.22.33              3116 pps   34.8 mbps      2 flows
159.11.22.33              2567 pps   29.5 mbps      2 flows
159.11.22.33              2439 pps    1.8 mbps     76 flows
159.11.22.33              2364 pps    1.4 mbps     55 flows
159.11.22.33              2104 pps    1.5 mbps     19 flows
159.11.22.33              1938 pps    1.3 mbps     36 flows

Outgoing traffic        225121 pps   1905 mbps  17893 flows
159.11.22.33              3699 pps   39.9 mbps     83 flows
159.11.22.33              3557 pps   37.3 mbps    124 flows
159.11.22.33              2965 pps   32.8 mbps     98 flows
159.11.22.33              2645 pps   29.7 mbps     38 flows
159.11.22.33              2522 pps   26.1 mbps     65 flows
159.11.22.33              2474 pps   26.8 mbps     61 flows
159.11.22.33              2285 pps   18.9 mbps    194 flows

Internal traffic             0 pps      0 mbps

Other traffic               56 pps      0 mbps

Traffic calculated in:  0 sec 14670 microseconds
Packets received:       2308537
Packets dropped:        0
Packets dropped:        0.0 %
```

Under Attack

- Announce BGP to UTRS from Team Cymru
- Simply Blackhole
- Run a shell/php/python/perl/whatever script
  - Connect to mikrotik router and run some commands
  - Connect to my cisco run ….
  - Just email or sms or telegram to me
- Announce BGP to cloud mitigation provider
- BGP flow spec/RFC 5575 (selective traffic blocking: GoBGP, ExaBGP)
- Save the tcpdump pcap file for later analyze

Thank You

Questions ?