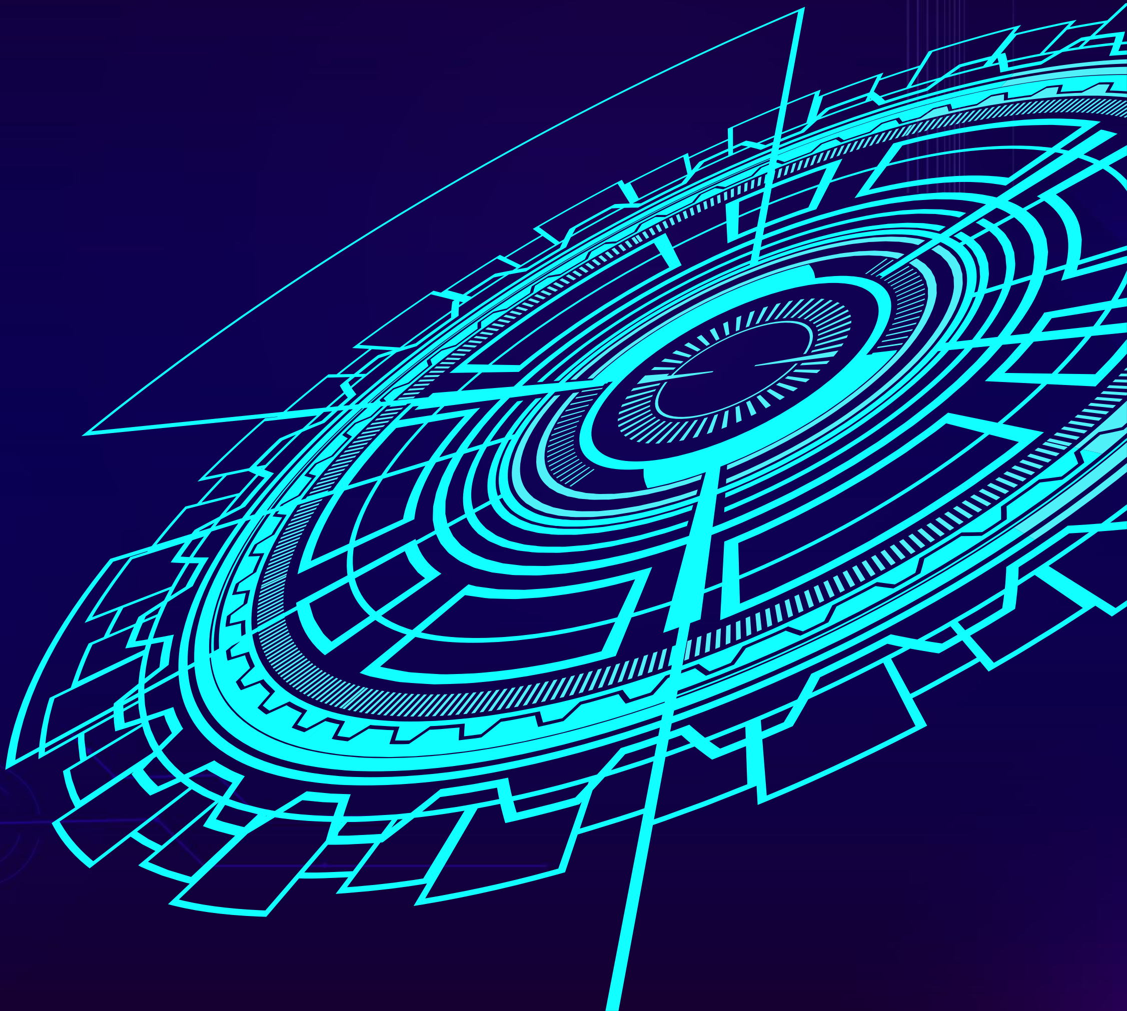
Network Telemetry

For DDoS Detection Applications



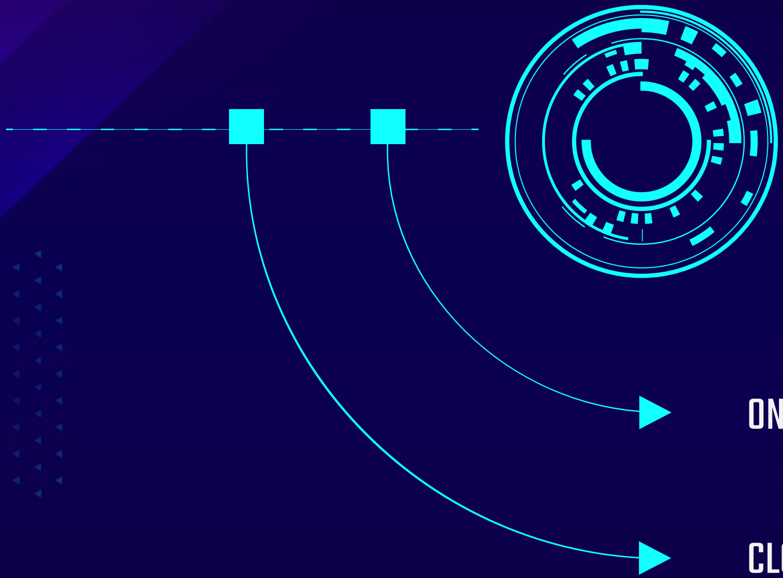
About me

I’m Pavel Odintsov, the author of open source DDoS detection tool, FastNetMon: https://github.com/pavel-odintsov/fastnetmon

Ways to contact me:

- linkedin.com/in/podintsov
- github.com/pavel-odintsov
- twitter.com/odintsov_pavel
- IRC, FreeNode, pavel_odintsov
- pavel.odintsov@gmail.com

Network Telemetry Types



ON PREMISE

CLOUD

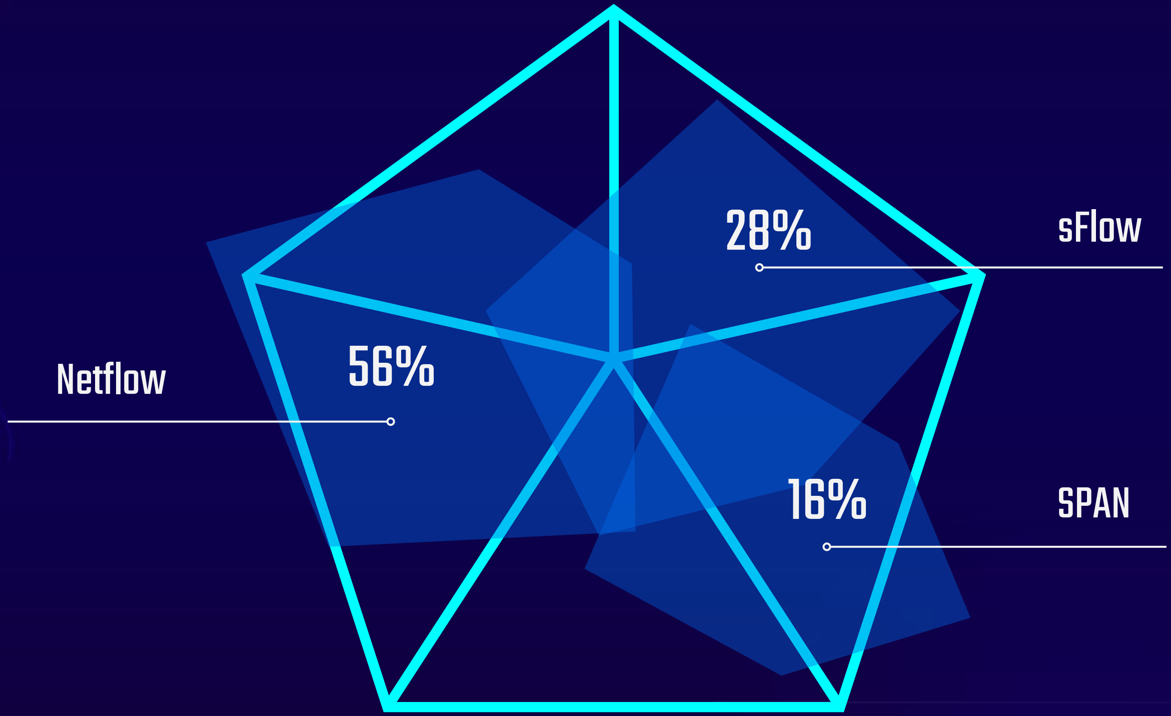
On Premise Telemetry

Netflow, IPFIX

sFlow

SPAN

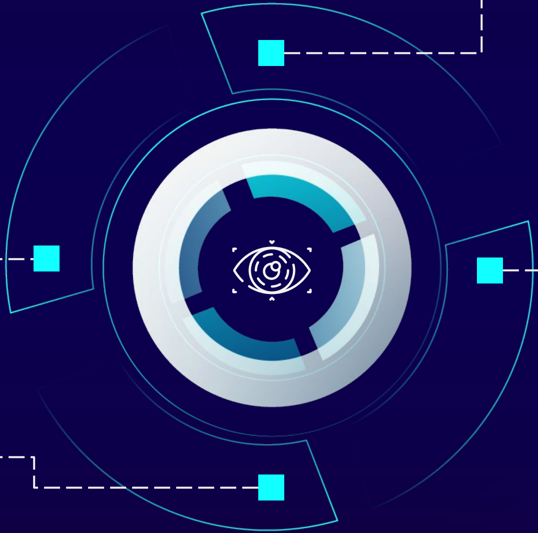
Protocols Use For DDoS Detection



Netflow Based Protocols

IPFIX, Netflow v5, Netflow v9, Netstream, jFlow, cFlow
and many others

Netflow Issues



Significant delay

Caused by flow aggregation engine, varies from 3 seconds up to 90 seconds

Scalability issues

Flow processing engine on many routers has very limited CPU power and constrained by flow table size

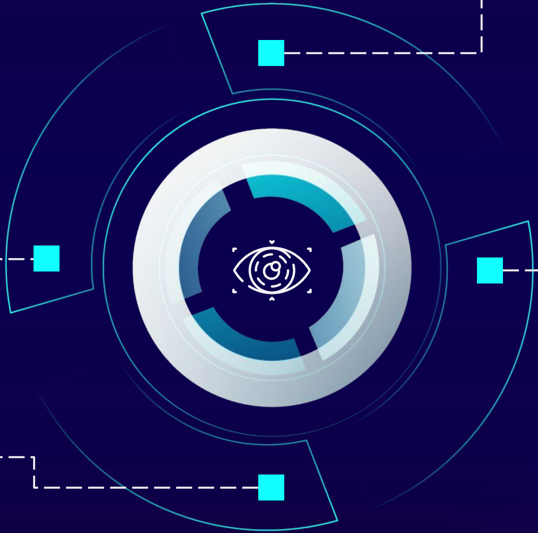
Lack of details

For effective DDoS detection we need fragmentation flags, TTLs and even part of payload

SAMPLING RATE REPORTING

Netflow based protocols use very complex way to encode sampling

sFlow Benefits



Very small / no delay

sFlow agents do not implement aggregation and they keep traffic only for very short period of time

Small CPU overheader

sFlow does not implement any kind of aggregation and does not need very efficient memory for flow tables

Keeps 60+ bytes from packet

Provides such important flags as TTL and fragmentation fields accompanied by first bytes of payload

Simple encoding protocol

Sampling rate is encoded directly in each packet, packet headers exported as-is without encoding

Vendors Do sFlow Wrong

Inadequate sampling rate

Many vendors limit minimum sampling rate by extremely harsh values (1:16000) which makes reliable attack detection impossible.

Scalability issues

In many cases due to slow CPU on control plane sFlow agent cannot export all traffic. Many hardware platforms have very limited capacity towards data plane

Lack of sFlow support

Only small subset of router vendors offer sFlow support and for few of them it just does not work well

Linux Traffic Capture

AF_PACKET

Available in all Linux distributions (excluding CentOS/RHEL 6)

AF_XDP

Available since Linux Kernel 4.19. Ubuntu 20.04 and later

Other

DPDK, Netmap, PF_RING, SnabbSwitch

Best Protocol For DDoS detection?

sFlow

Cloud Network Analytics

Amazon VPC Flow logs

Limited by 60 second delay, expensive and complex way to export logs

Google Flow Logs

Limited by UDP and TCP traffic only, expensive and complex way to export logs

Azure Flow Logs

Excellent visibility with Network Traffic Watcher instrument

THANKS

Any questions?

pavel.odintsov@gmail.com

🐦 @odintsov_pavel

in linkedin.com/in/podintsov