Root Cause Analysis

benefits of having Flow data right beside SNMP

FLOWCUTTER

Mgr. Matej Pavelka PhD.

Lessons learnt from 2 use cases

- #1 case
- #2 case
- Best practices

#1 case

Latency issue at SME customer

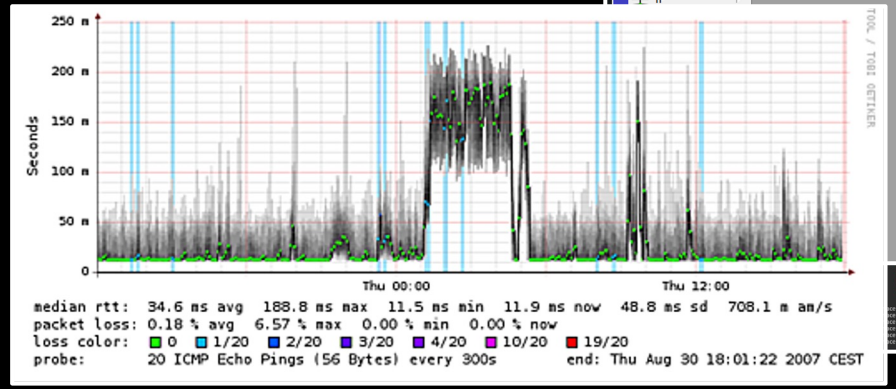
FLOWCUTTER

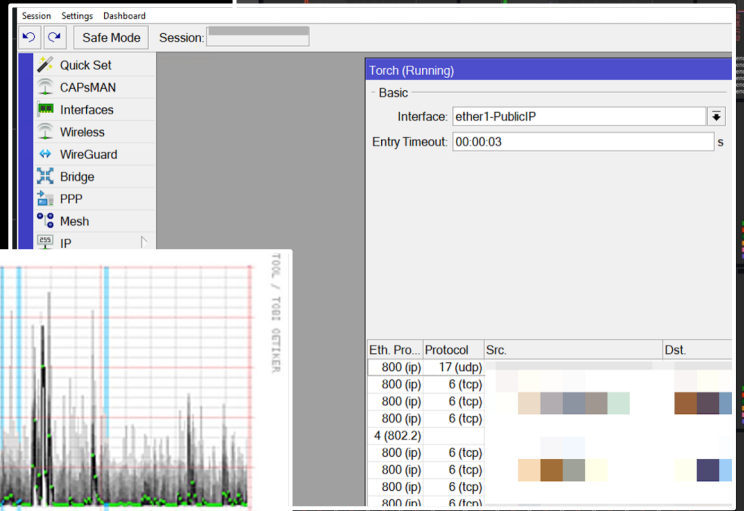
Anomaly

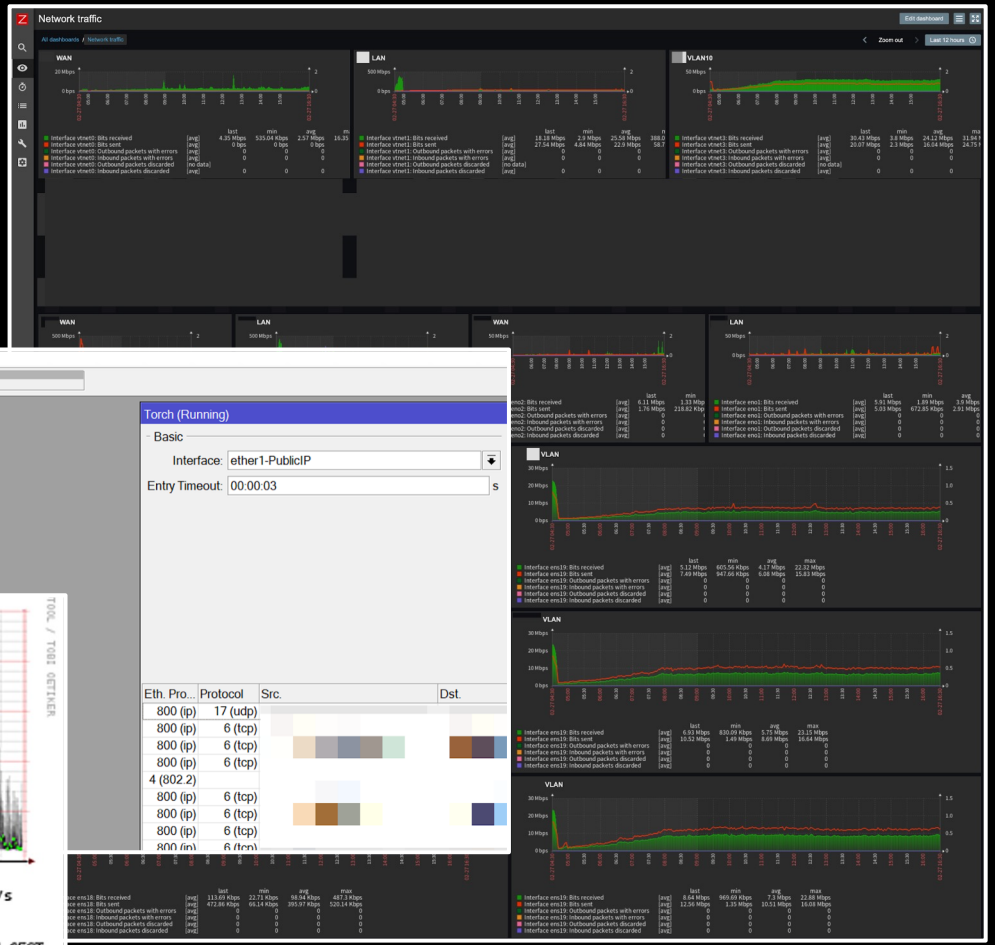
- Latency and connection issues
- For ~10 minutes
- Every ~1.5h

#1 ISP stack

- Zabbix
- Mikrotik winbox
- Smoke ping



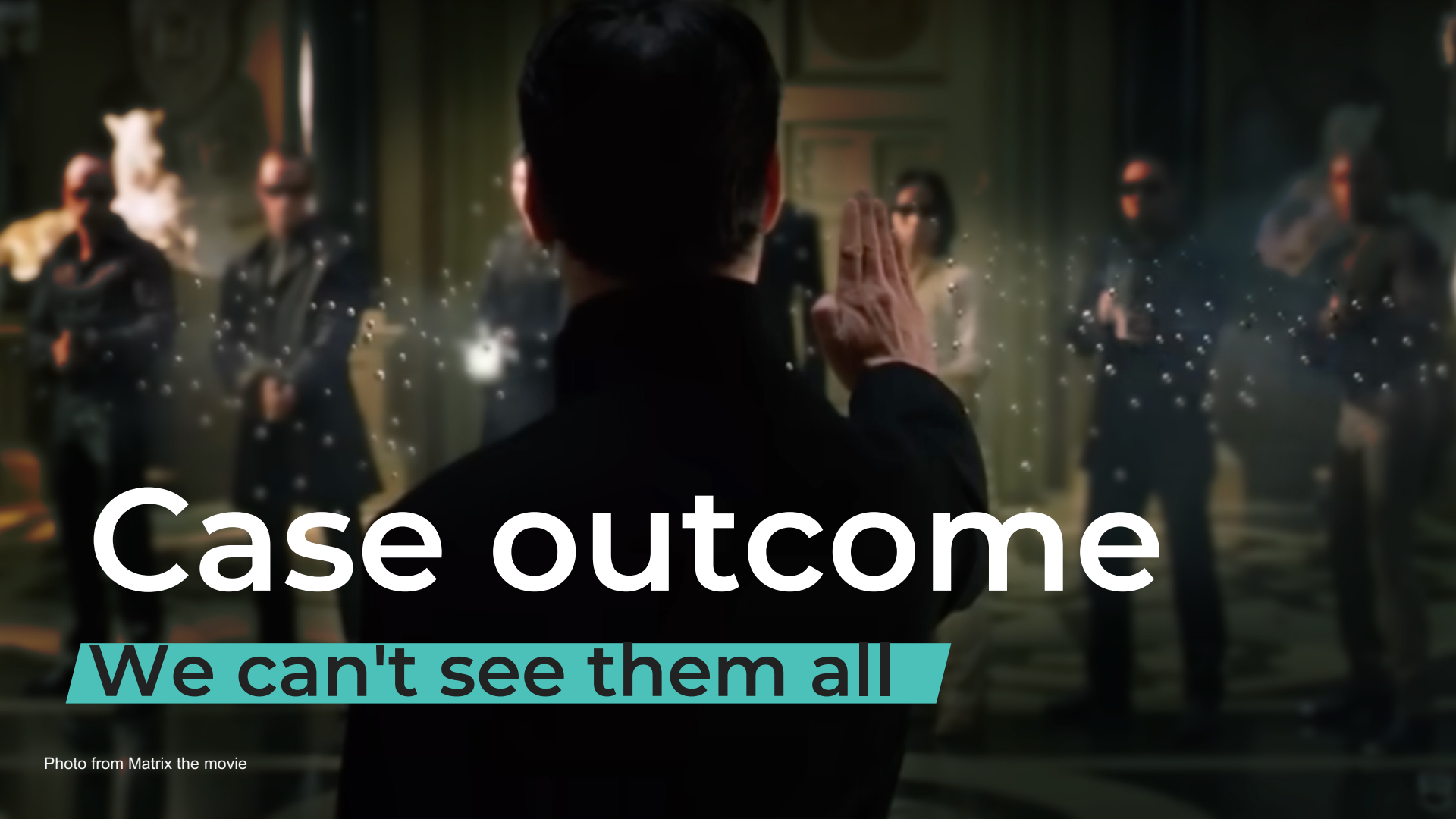




FLOWCUTTER

Outcome

- Customer experienced low quality service.
- ISP wasn’t able find root-cause or mitigate it.
- ISP’s reputation was hit.



Case outcome

We can't see them all

Photo from Matrix the movie

#2 case

?

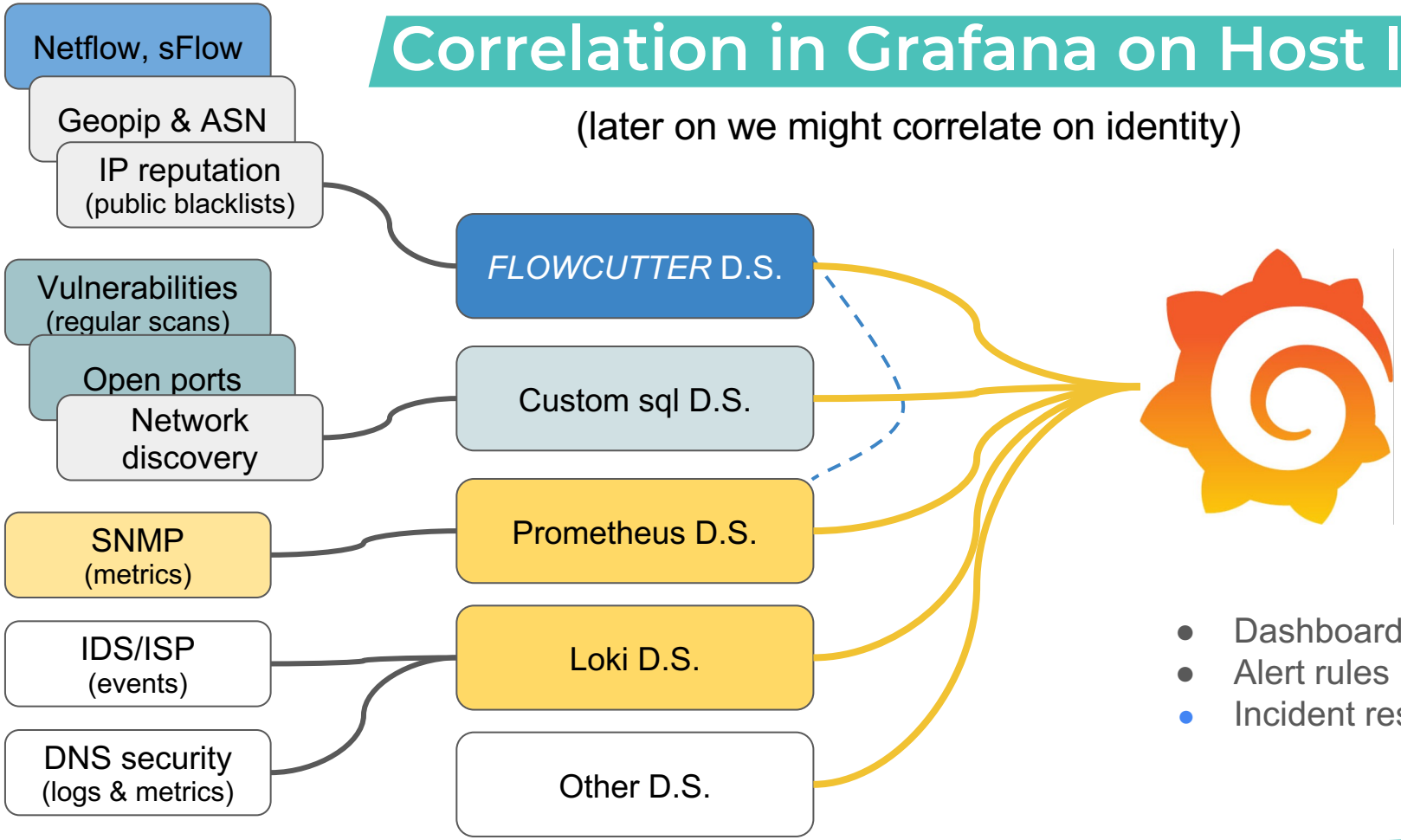
FLOWCUTTER

#2 ISP - Monitoring stack

- **Grafana UI**
- **Data sources**
  - **SNMP** (Prometheus)
  - **Flows** (FLOWCUTTER)
  - **Vulnerability and open ports**
  - No DNS security data (unfortunately)

Correlation in Grafana on Host IP

(later on we might correlate on identity)



- Dashboards
- Alert rules
- Incident response

Morning's Alert

- **Alert fired 11:46**
- **P95 latency**
- **On CORE router #14** (of 31)

Router #14	10G uplink both SME and home connections 22 downstream 1G links

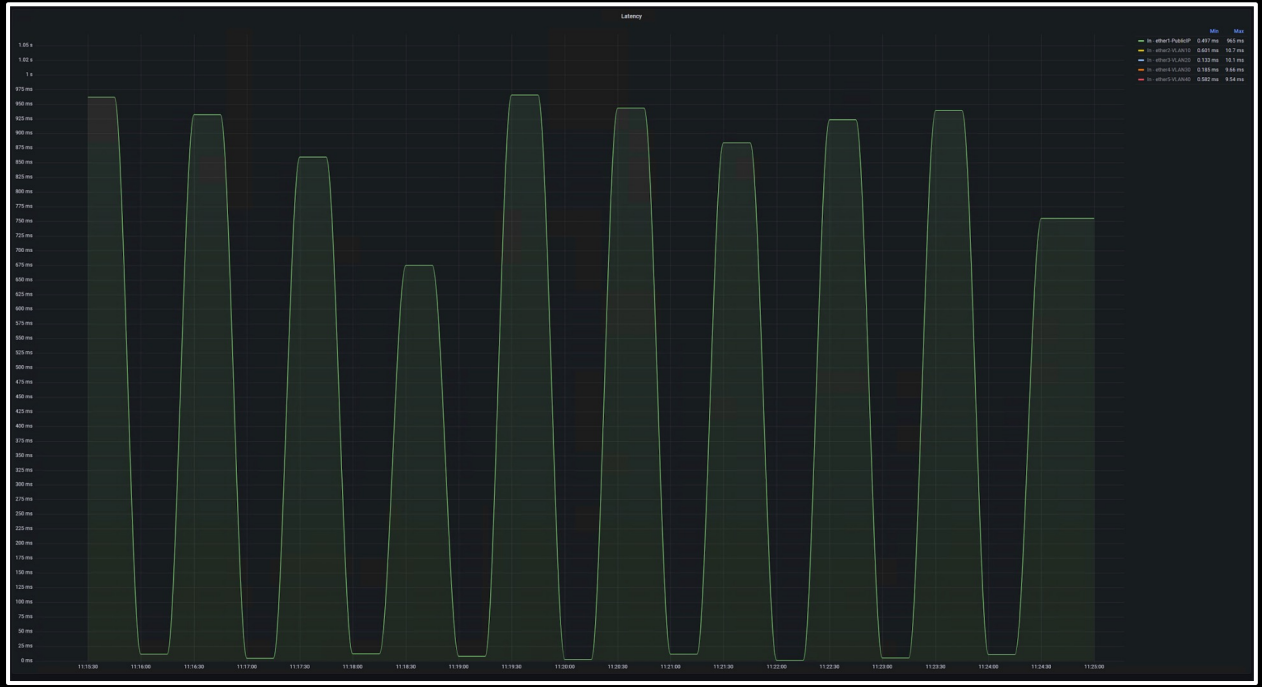
Specialized dashboard

- Out of the box
- Any vendor
- For each CORE router

FLOWCUTTER

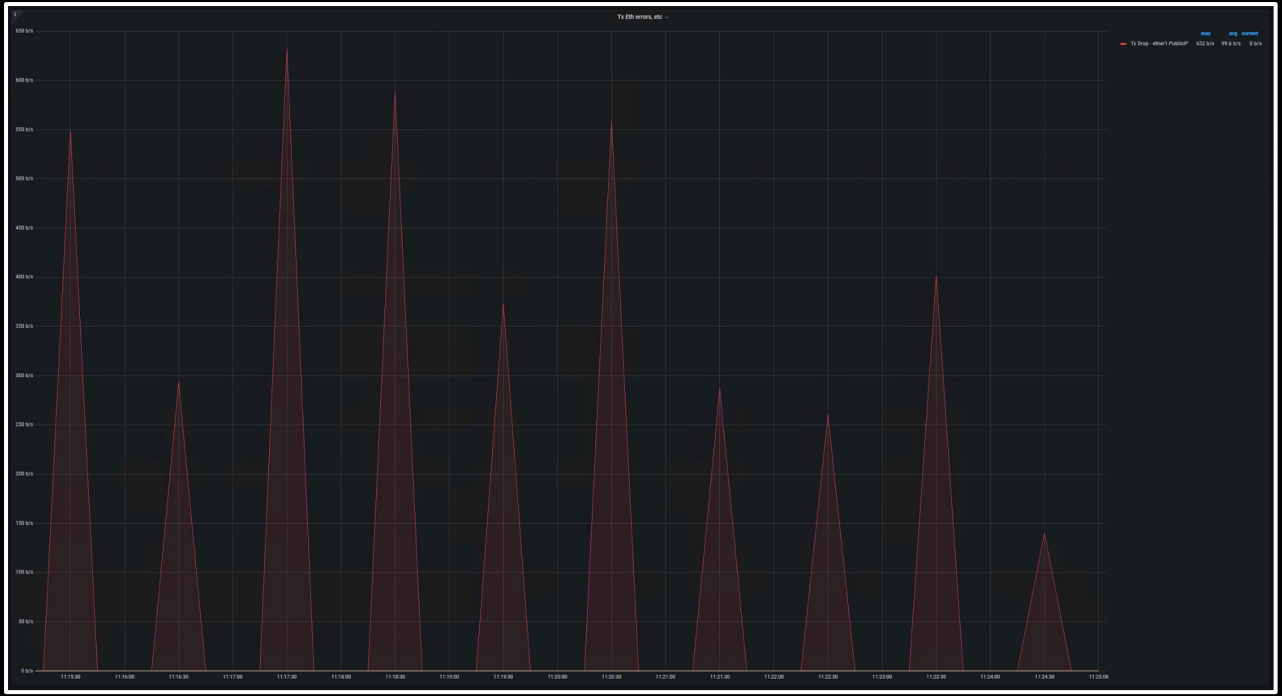
Latency on #14

- 11:45 10 minutes



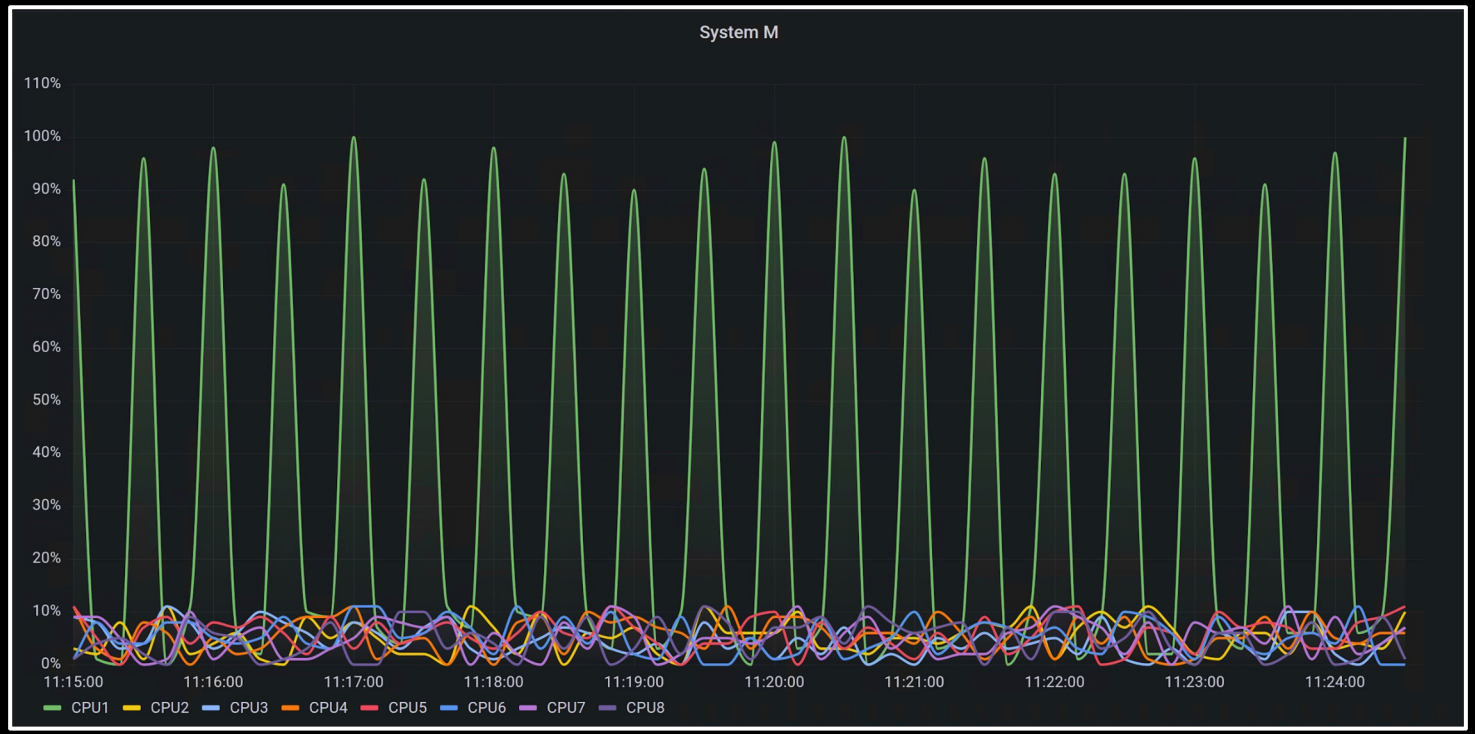
Packets dropped

- 11:45 10 minutes



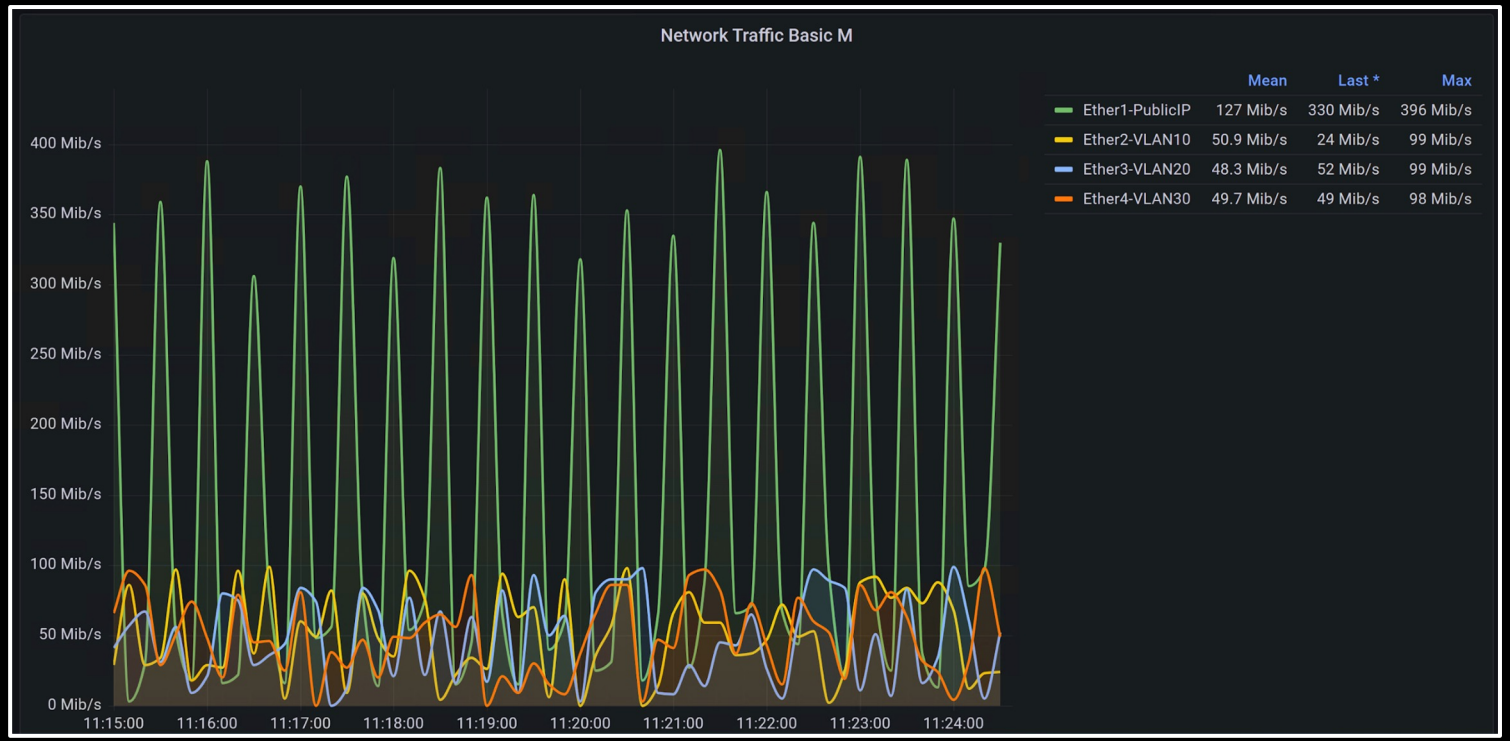
CPU on router

CPU 1



Traffic on port

One eth port w/ peaks in bps



SNMP x Flows

- SNMP - 1D dimensional time series
- Flows - high-cardinality big data

netflow

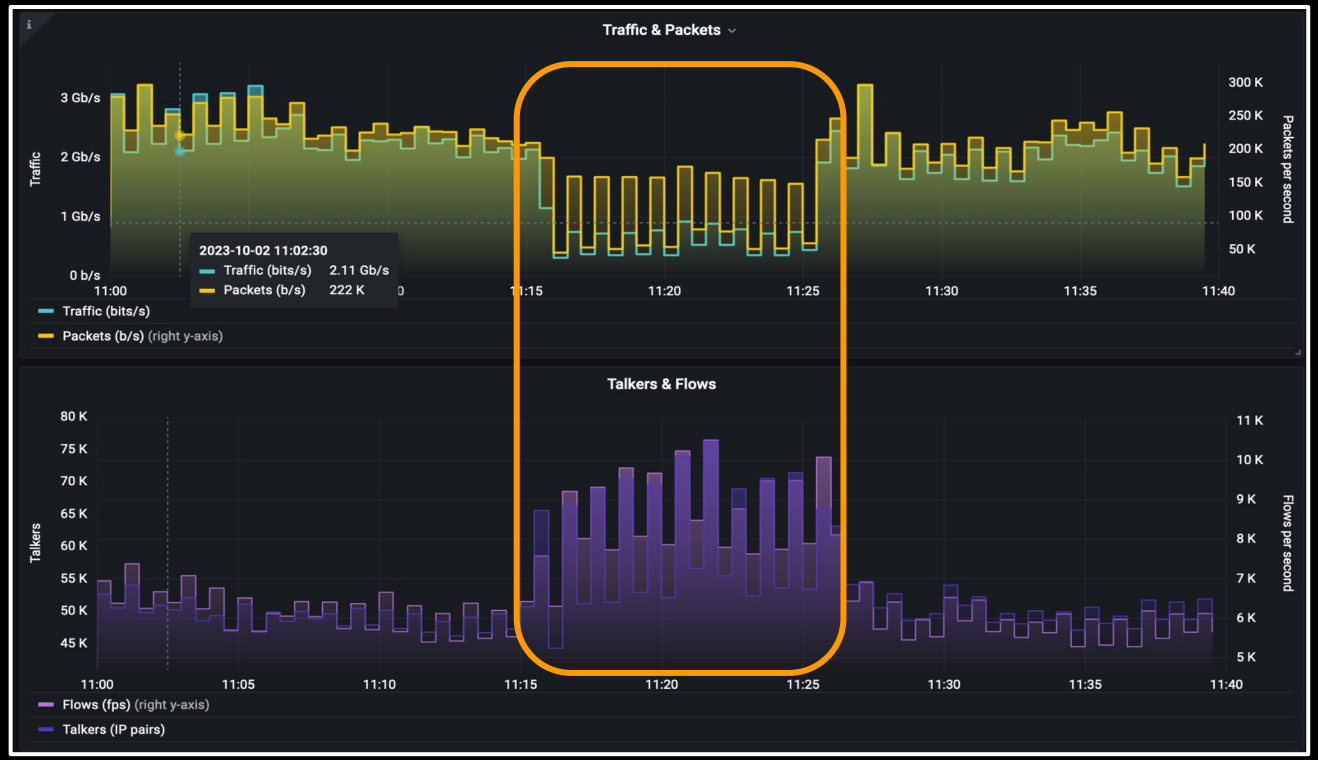
analýza

Phto from Matrix the movie

FLOWCUTTER

ISP traffic

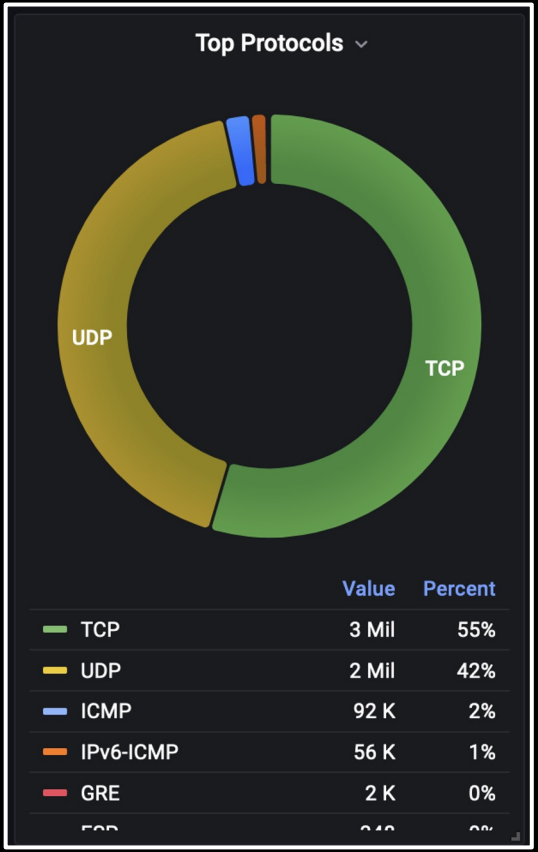
All traffic BPS, PPS, FPS, talkers



10 minutes

Drill down

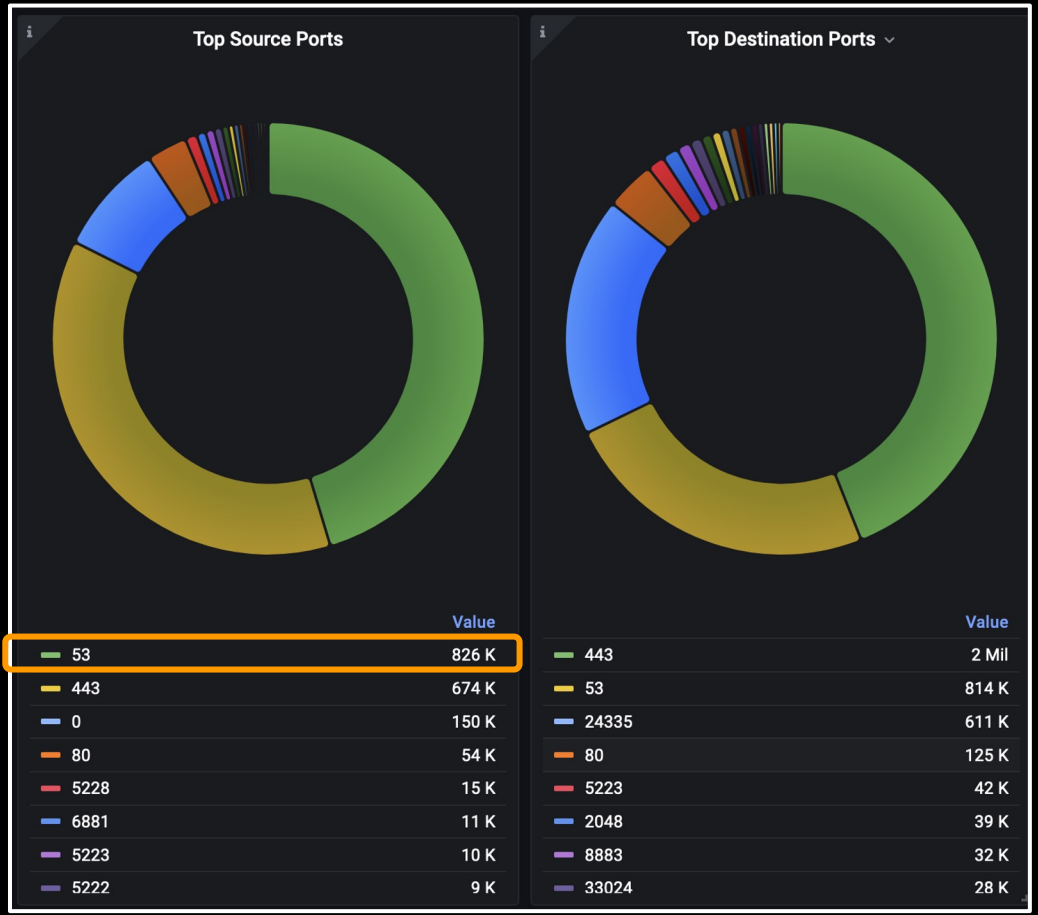
- Protocols are OK



	Value	Percent
TCP	3 Mil	55%
UDP	2 Mil	42%
ICMP	92 K	2%
IPv6-ICMP	56 K	1%
GRE	2 K	0%

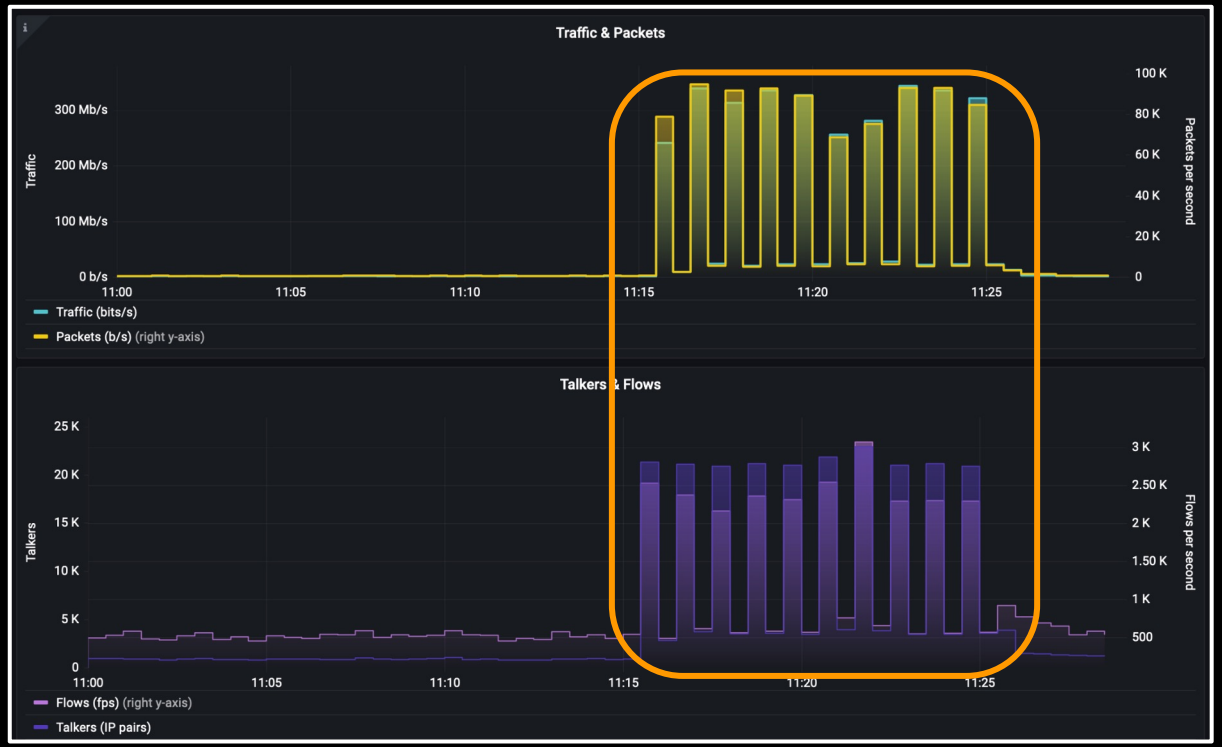
Drill down

- DNS responses
- Source port = 53



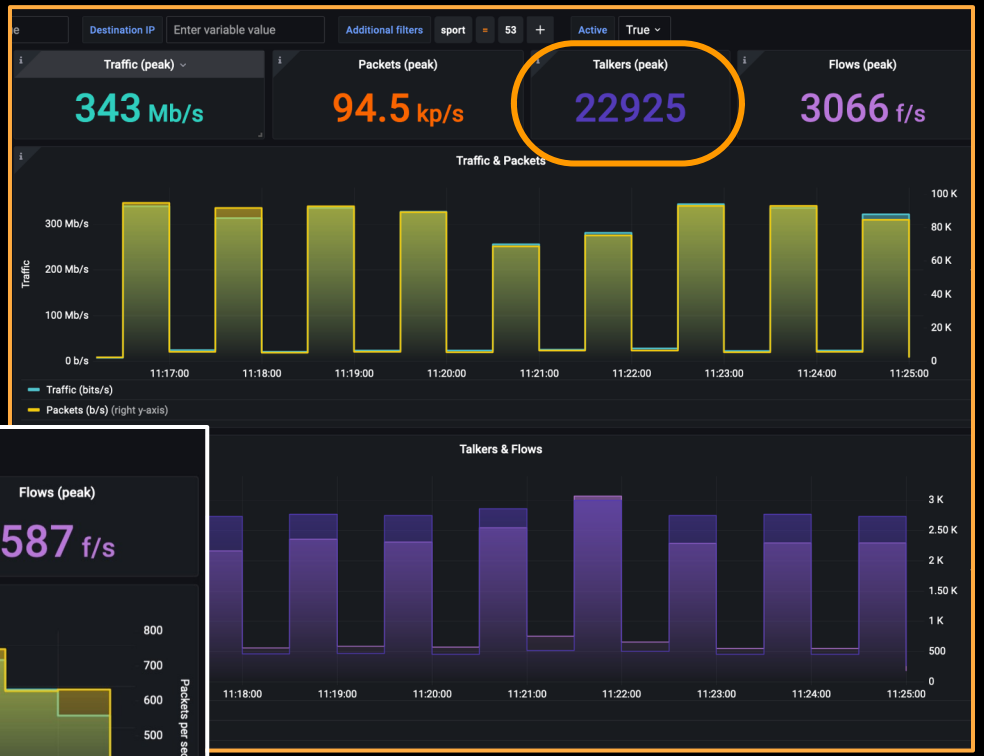
DNS responses

Filtered source_port = 53

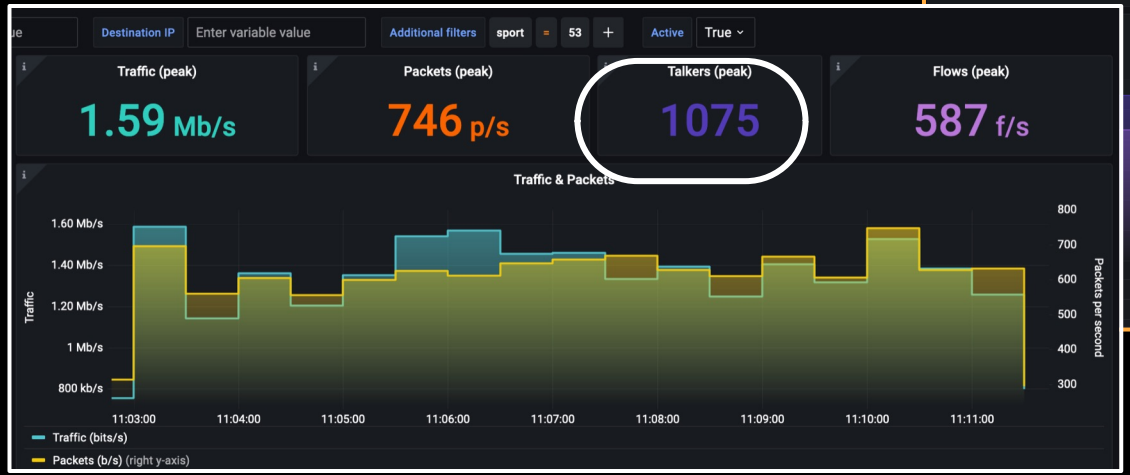


Before / after

During DDoS attack

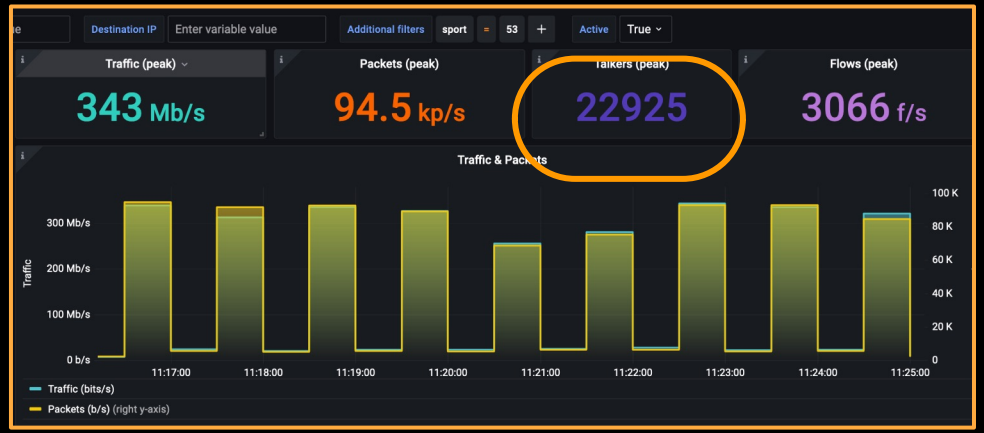


Before DDOS



Reflection attack

- Distributed attack on DNS
- Src/Dest ports = 53/24335



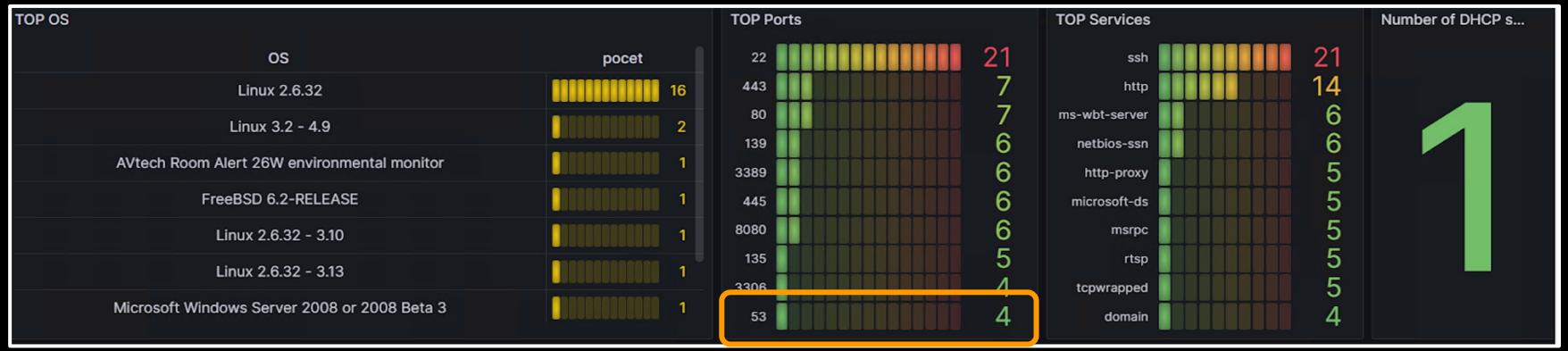
Mitigation

- **Using BGP Flowspec** (RFC 5575)
- **Granular control** (compared to RTBH)
  - s/d port
  - packet length
  - TCP flags
  - ICMP code
  - etc...

Open ports

- **Automated scan** (every night)
- **DNS port open** on SME customer's public IP

Example screenshot (not the actual case)



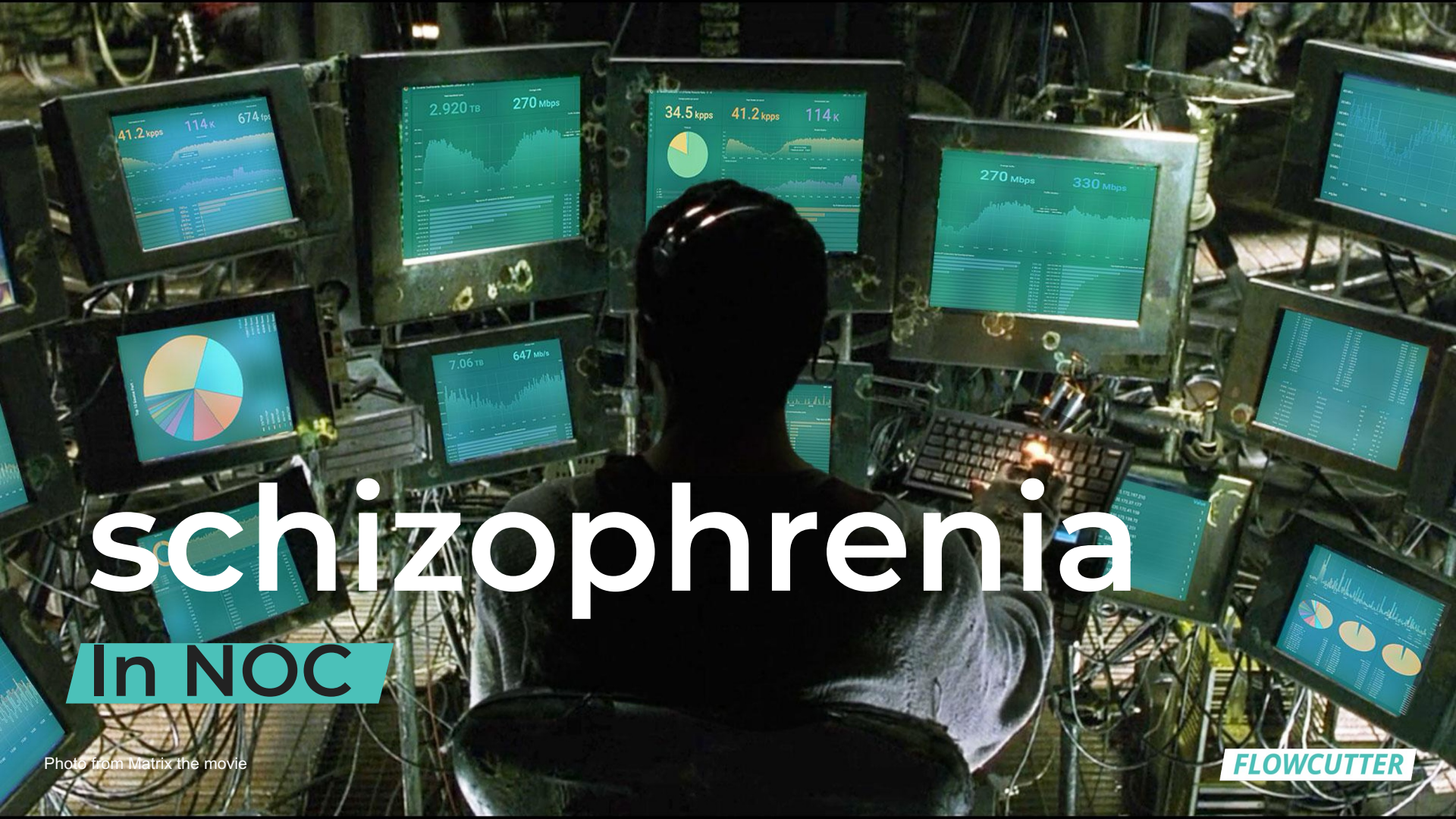
Outcome

- ISP was able to detect anomaly and find root-cause.
- ISP mitigated it before customer called.
- ISP’s admin found misconfiguration of customer’s DNS resolver and informed them.

Photo from Matrix the movie

5 Best practices

- **One ⬡ to rule them all** (OSS, no vendor lock, incident response)
- ???
- ???
- ???
- ???



schizophrenia

In NOC

Photo from Matrix the movie

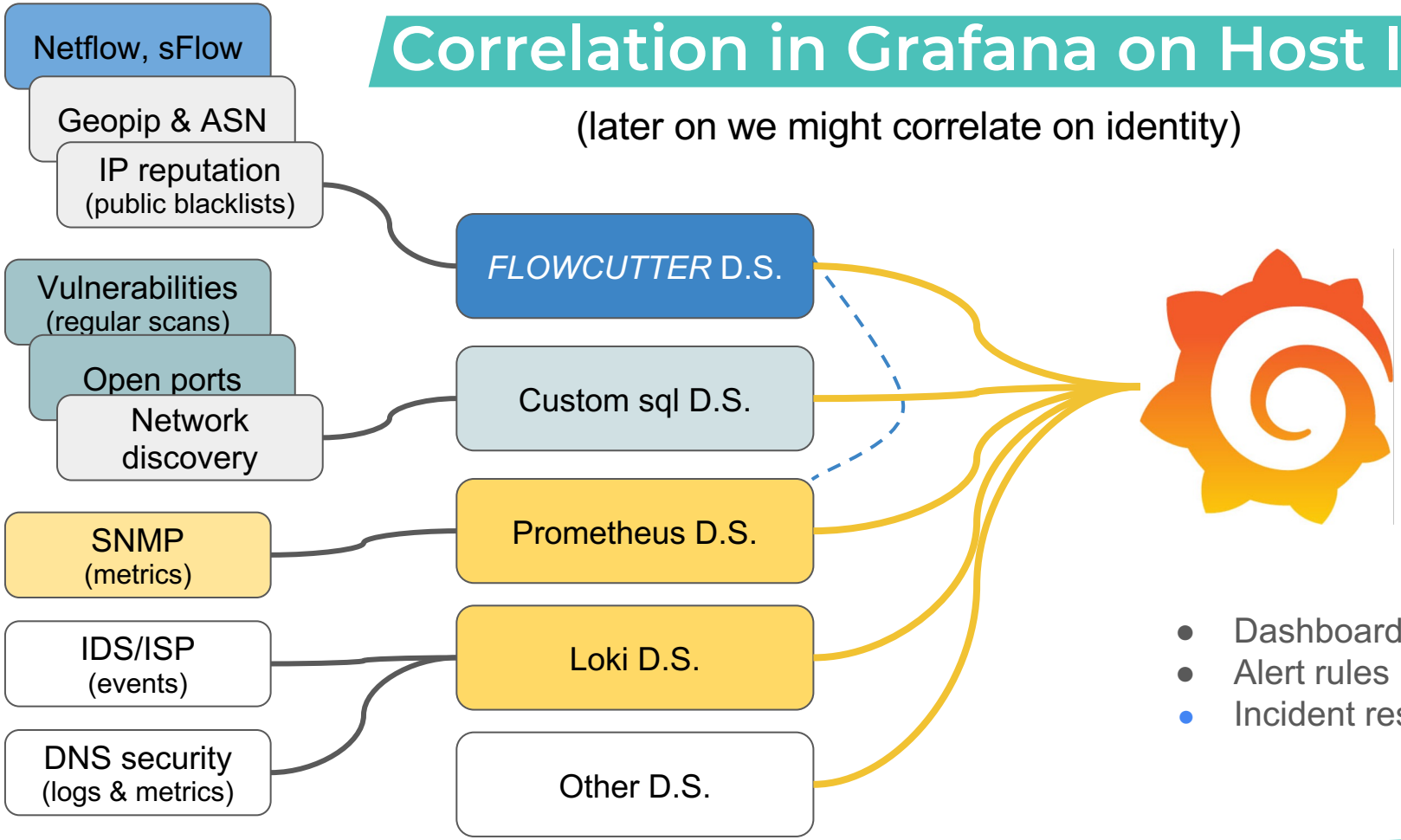
FLOWCUTTER

Putting it all together in Grafana

FLOWCUTTER's approach

Correlation in Grafana on Host IP

(later on we might correlate on identity)



- Dashboards
- Alert rules
- Incident response

5 Best practices

- One ⬡ to rule them all (OSS, no vendor lock, incident response)
- Well labeled SNMP metrics
- ???
- ???
- ???

5 Best practices

- One ⬡ to rule them all (OSS, no vendor lock, incident response)
- Well labeled SNMP metrics
- Fast & Furious flows
- ???
- ???

netflow

analýza

Phto from Matrix the movie

FLOWCUTTER

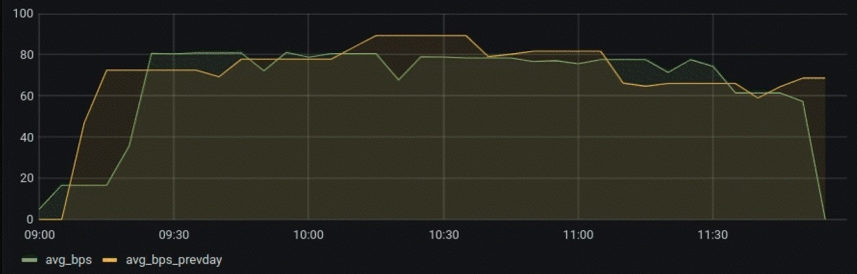
site all filter +

Panel Title

Search:

sport	dport	proto	stime	etime
546.00	547.00	UDP	2021-06-02 11:24:43.982000	2021-06-02 11:54:40.440000
546.00	547.00	UDP	2021-06-02 10:54:32.508000	2021-06-02 11:24:13.178000
546.00	547.00	UDP	2021-06-02 10:24:24.670000	2021-06-02 10:54:24.572000
546.00	547.00	UDP	2021-06-02 09:53:38.573000	2021-06-02 10:23:25.106000
546.00	547.00	UDP	2021-06-02 09:23:31.083000	2021-06-02 09:52:57.031000

Panel Title

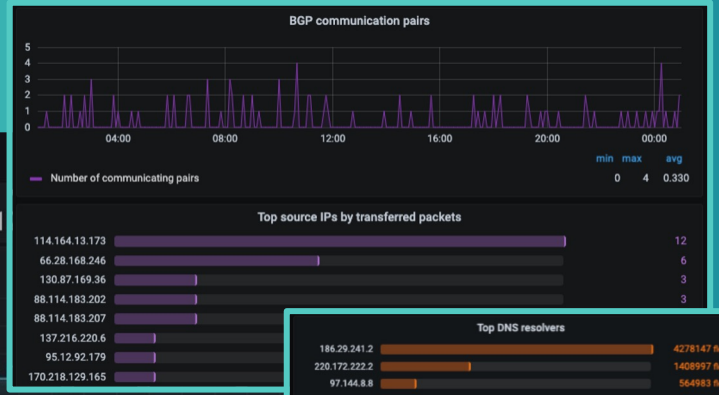


Panel Title

	Value
213.195.223.16/UDP	2 Mil
81.30.226.13/UDP	2 Mil
213.195.223.14/UDP	2 Mil
81.30.226.12/UDP	1 Mil
81.30.226.14/UDP	1 Mil
217.66.163.24/UDP	1 Mil
157.240.30.21/UDP	1 Mil
157.240.30.63/UDP	1 Mil
213.195.224.131/UDP	969 K
81.30.241.154/UDP	881 K
213.195.224.212/UDP	797 K
213.195.223.59/UDP	739 K
94.230.149.146/UDP	732 K
213.195.194.185/UDP	720 K
35.214.151.58/UDP	644 K
213.195.223.10/UDP	620 K
213.195.222.222/UDP	588 K
217.66.163.108/UDP	577 K
213.195.223.30/UDP	556 K
213.195.205.168/UDP	541 K

FLOWCUTTER

Grafana examples



FLOWCUTTER

5 Best practices

- One ⬡ to rule them all (OSS, no vendor lock, incident response)
- Well labeled SNMP metrics
- Fast & Furious flows
- Export Metrics from flows (to Prometheus, Zabbix, Influxdb)
- ???

vendor lock

Zabbix, Grafana, ...

Photo from www.geocaching.com

FLOWCUTTER

5 Best practices

- **One ⬡ to rule them all** (OSS, no vendor lock, incident response)
- **Well labeled SNMP metrics**
- **Fast & Furious flows**
- **Export Metrics from flows** (to Prometheus, Zabbix, Influxdb)
- **Cloud or On-prem**

Thank you,

ques-tions?

Mgr. Matej Pavelka PhD.

www.flowcutter.com