

FLOWCUTTER

Nástroj na Analýzu Netflow

Mgr. Matej Pavelka PhD.

FLOWCUTTER

Troubleshooting / Analýza problému

Když je problém, chci znát rychle odpověď

Nemám křišťálovou kouli



FlowCutter

Nástroj na **vizualizaci a analýzu** syrových **flow dat**

Nejrychlejší a Škálovatelný

Otevřený (API)

a ohnutelný K obrazu svému



FLOWCUTTER

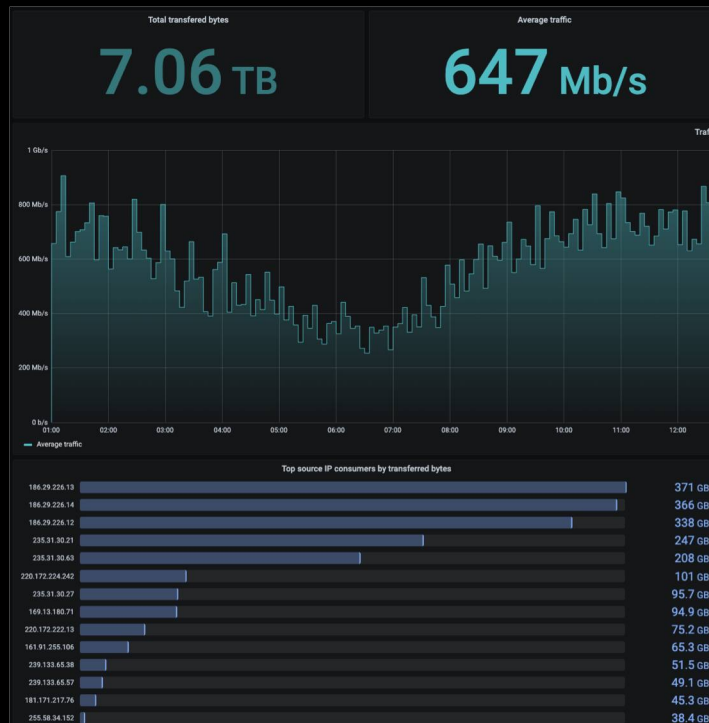
Bandwidth Utilization

Total transferred bytes

7.06 TB

647 Mb/s

Average traffic for a given segment



Traffic during the day

Top 100 consumers by source IP

FLOWCUTTER

Filtering

E.g. by source IP address CIDR

Site	Lhota - Perimet ▾	Source IP	1.2.3.4/23	Destination IP		Active	True ▾
------	-------------------	-----------	------------	----------------	--	--------	--------

FlowCutter allows filtering by any IPFIX field

You can create even complex queries

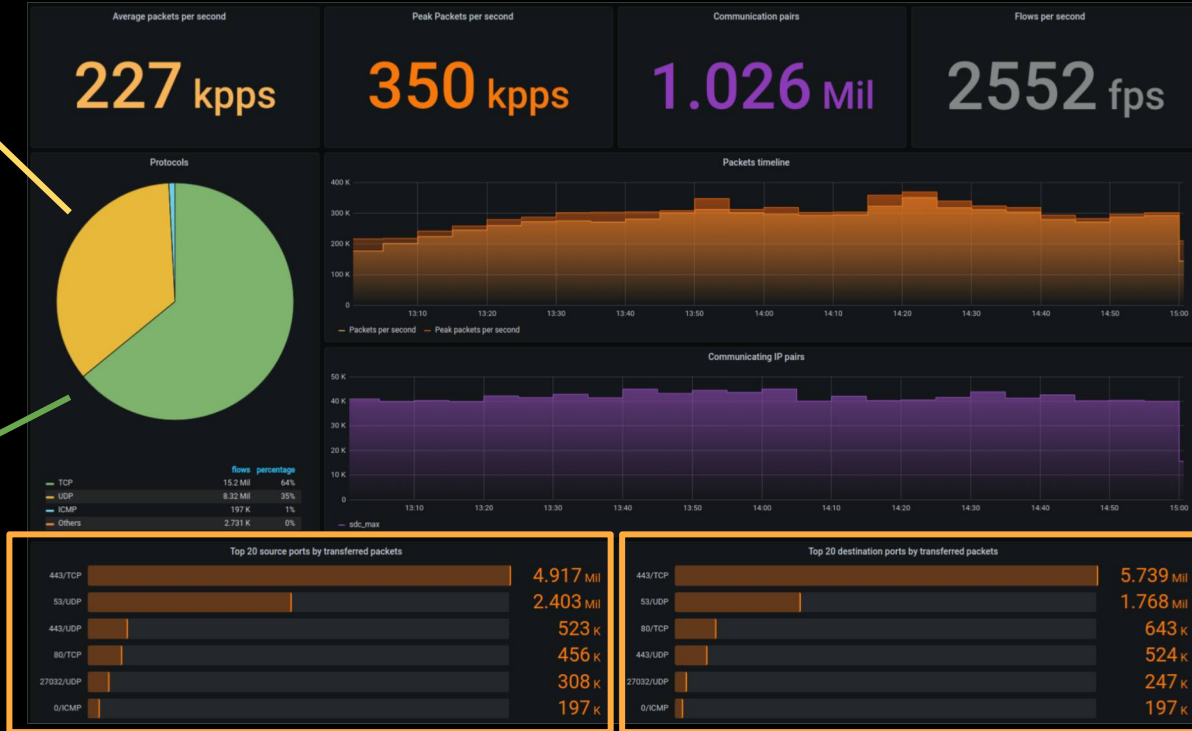
FLOWCUTTER

Ports and Protocols (L4 L5)

UDP

TCP

Top 20
Source Ports



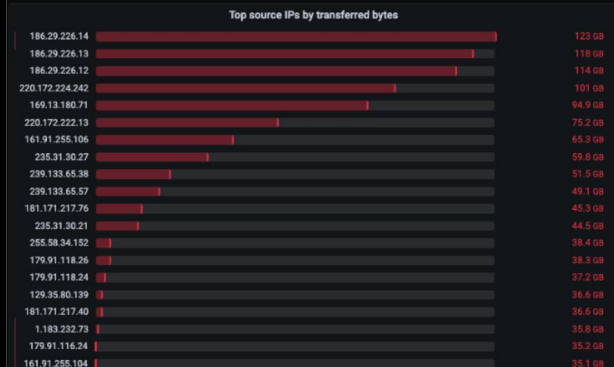
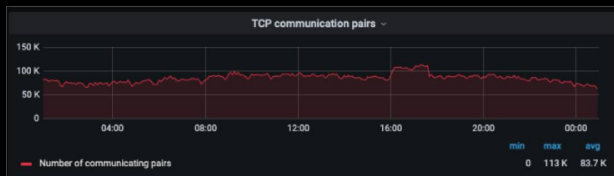
Top 20
Dest. Ports

FLOWCUTTER

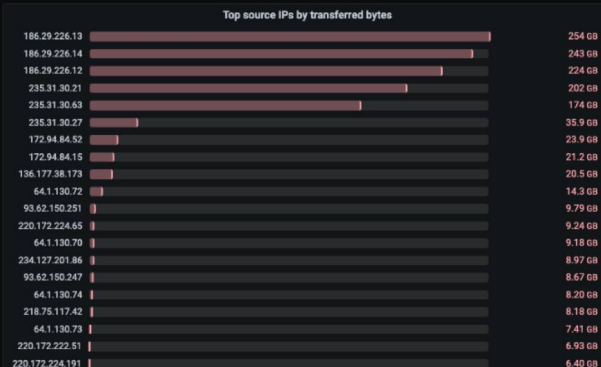
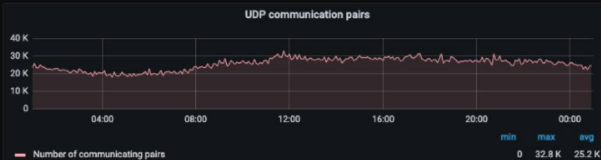
FLOWCUTTER

TCP vs UDP vs ICMP

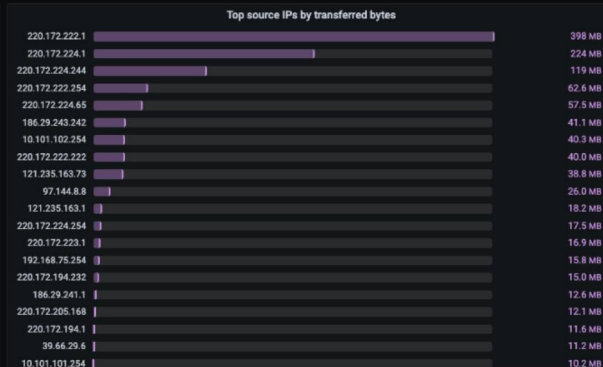
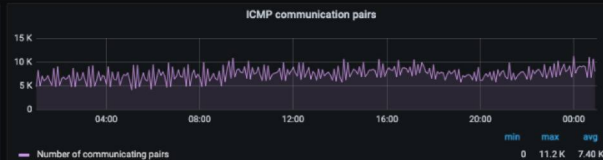
TCP



UDP



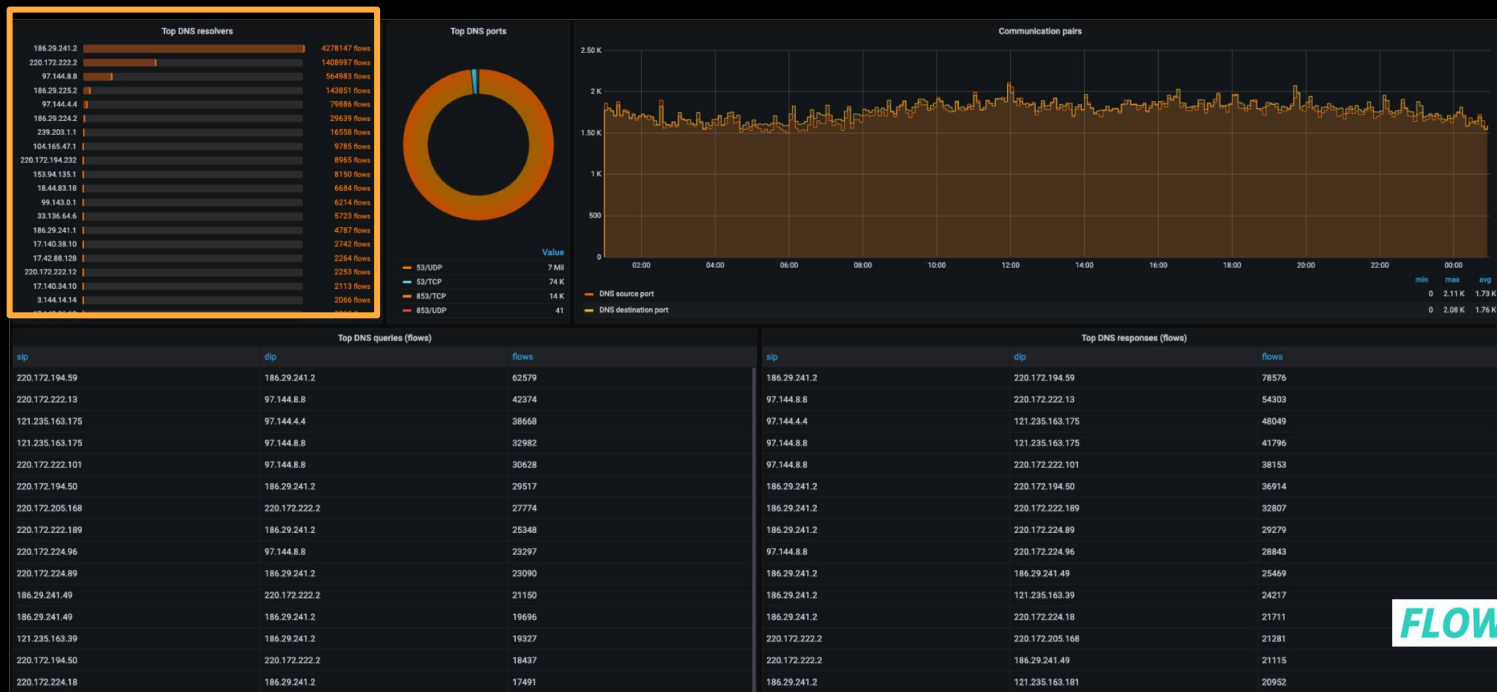
ICMP



FLOWCUTTER

Visibility to your DNS resolvers

Top DNS Resolvers (by flows)



“K obrazu svému”

Grafana + FlowCutter datasource

umožňují

- Vlastní dashboardy
- Vlastní vizualizace / grafy

Několik **užitečných dashboardů** je předinstalovaných.



FLOWCUTTER

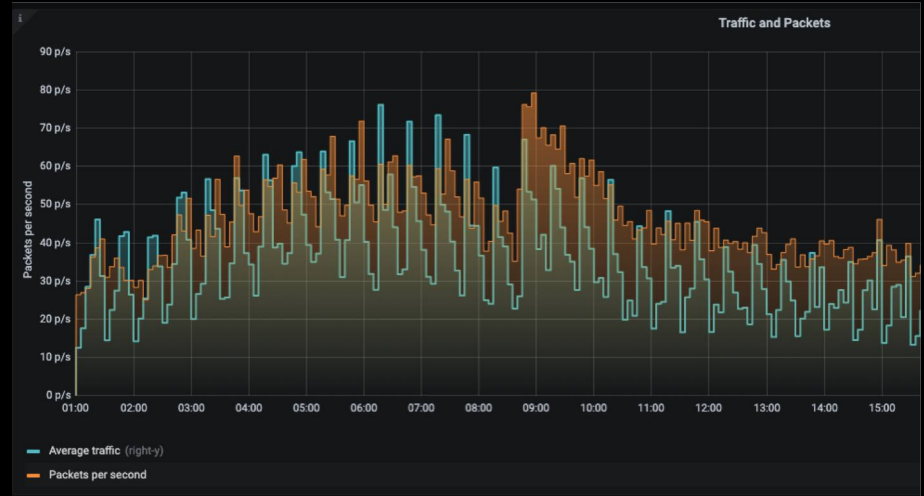
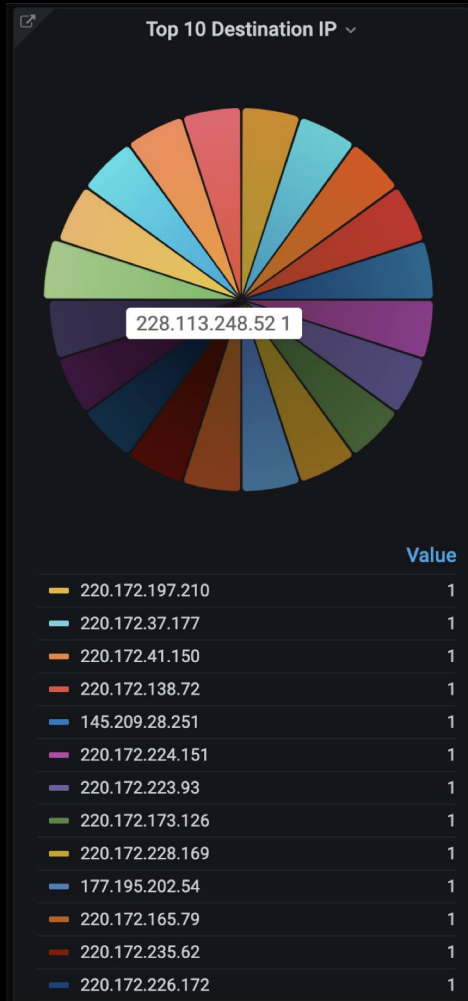
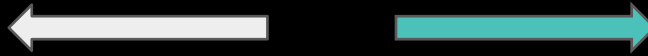
Filter, and quick check download/upload



FLOWCUTTER

FLOWCUTTER

Scanners and bots examples



FLOWCUTTER

Nástroj na vizualizaci a analýzu syrových flow dat

+ *Nejrychlejší*

+ *K obrazu svému*

+ *Otevřený*

FLOWCUTTER

Chcete zkusit?

matej.pavelka@flowcutter.com

FLOWCUTTER