Maxifi

maximize your wi-fi network

Maxifi NetFlow Explorer

Jiří Zelenka / Radim Dolák

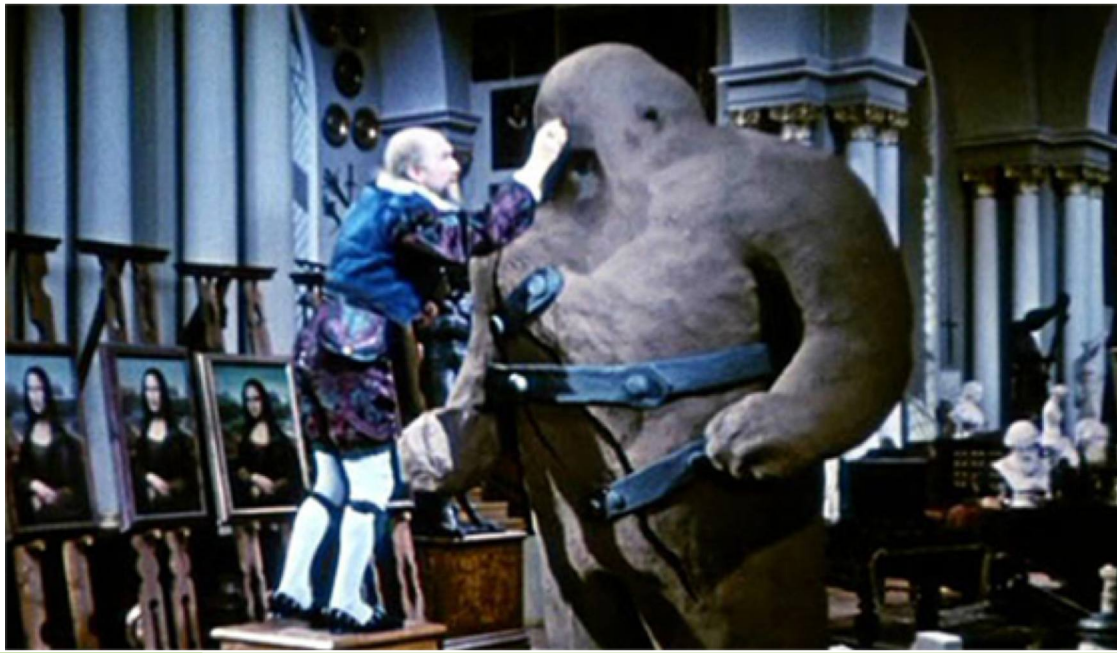
Ten dělá to a ten zas tohle …

Ne vždy je nutné vymýšlet Golema…

Maxifi
maximize your wi-fi network

Golém nebo „Šém“ ?

- Veliké úsilí k vytvoření Golema nevede bez „Šému“ k úspěchu
- Je pro vás efektivní vytváření Golemů nebo je lepší nalézt „Šém“ a správně jej vložit do vaší sítě
- Využijte od každého to, co umí nejlépe
- Vložte „Šém“ do vaší sítě a svůj čas věnujte jejímu dalšímu rozvoji
- Ušetřete, rozvíjejte …



Maxifi NetFlow Explorer

Maxifi
maximize your wi-fi network

Maxifi NetFlow Explorer

- Sběr a interpretace NetFlow dat pomocí webového GUI
- Postaveno nad open source řešením nfdump
- Součást rodiny produktů Maxifi
- Určeno pro ISP i podnikové sítě
- Responzivní zobrazení
- Nezávislé na HW
- Podpora IPv4 i IPv6
- Provoz v ČR / SR

Maxifi
maximize your wi-fi network

Pro koho je NFE určeno ?

- Poskytovatelé připojení (ISP)
- Podnikoví zákazníci

Proč NFE potřebuji a v čem mi pomůže ?

- Vizibilita sítě a diagnostika problémů
- Sledování trendů i historie fungování přípojek
- Pomocník při bezpečnostních incidentech
- Splnění zákonné povinnosti ISP (data retention)

Maxifi
maximize your wi-fi network

NetFlow – co to přesně je ?

- Standardizovaný sběr dat o síťových spojeních
- Odkud, kam, kdy, kolik, čeho, jak …


```
"type" : "FLOW",
"sampled" : 0,
"export_sysid" : 1,
"t_first" : "2022-04-21T14:38:19.882",
"t_last" : "2022-04-21T14:38:19.882",
"proto" : 17,
"src4_addr" : "192.168.1.1",
"dst4_addr" : "205.251.194.85",
"src_port" : 34940,
"dst_port" : 53,
"fwd_status" : 1,
"tcp_flags" : ".....",
"src_tos" : 0,
"in_packets" : 1,
"in_bytes" : 104,
"input_snmp" : 37,
"output_snmp" : 38,
"src_as" : 0,
"dst_as" : 0,
"label" : "<none>"
```


CISCO

HUAWEI

MikroTik

Hewlett Packard Enterprise

Linux Operating System

WatchGuard

Maxifi
maximize your wi-fi network

Možnosti nasazení

Maxifi Cloud

- Řešení plně poskytováno formou služby
- Pro testování i menší instalace
- Důraz na zabezpečení přenášených dat
- Žádné vstupní náklady

Server „On premise“

- Provoz na zakoupeném dedikovaném serveru umístěném u zákazníka
- Robustní výkon za dostupnou cenu
- Citlivá data neopouští Vaši síť
- Vzdálená správa jako služba

Maxifi
maximize your wi-fi network

Přehledná interpretace NetFlow záznamů

- Kompletní a přesto jednoduchý přehled spojení
- Hledání konkrétního spojení
- Možnost využití filtrů
- Algoritmy korelace NetFlow dat
  - Spojení před a za NATem
  - Příchozí a odchozí spojení
  - Chybějící ASN, Country

Maxifi
maximize your wi-fi network

Proč nestačí “nfdump” ?

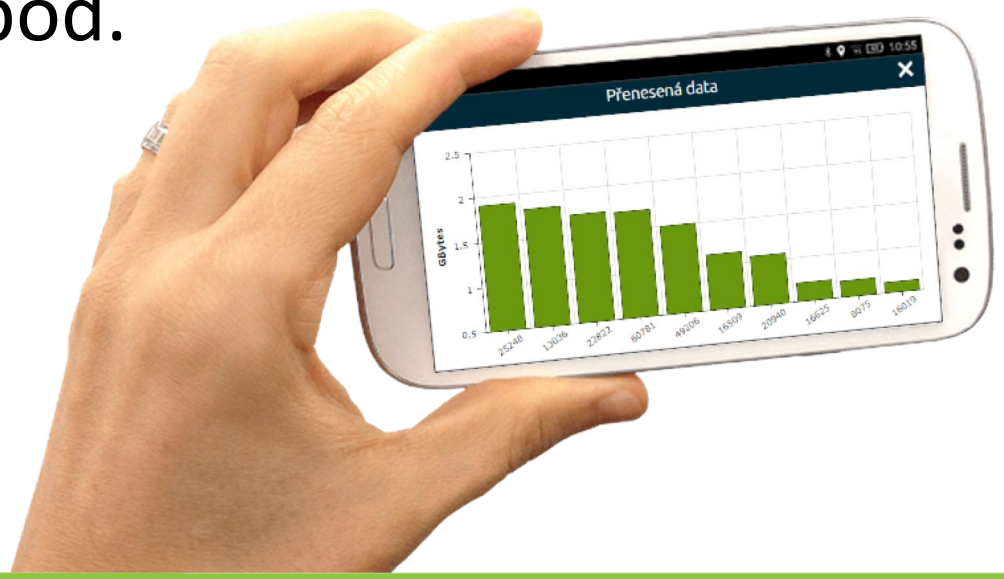
- Příkazový řádek je přeci fajn ….
  - Pro všechny a i z mobilu ?
  - Není lepší použít ten správný „Šém“ a šetřit čas i náklady?
- Jeden graf může vydat za tisíc čísel a slov

```
root@collector:/usr/local/maxifi/www/nfe/data/nfdump/2022-04-20# nfdump -r nfcapd.202204200950 -c 50 -B
Date first seen          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Out Pkt   In Pkt Out Byte   In Byte Flo
2022-04-20 09:54:35.893     0.025 TCP      10.115.88.250:55692 <->     165.225.26.43:80          3        0      293         0
2022-04-20 09:53:46.608    65.361 TCP       185.64.40.23:26440 <->    157.240.30.21:443         11       10     1366      1222
2022-04-20 09:50:14.744     2.151 TCP       185.64.41.74:49974 <->   17.248.172.105:443         25       22     9912      7734
2022-04-20 09:49:34.875     0.944 UDP        10.115.70.2:61696 <->     95.101.36.64:53          1        1      154       101
2022-04-20 09:53:42.799     1.143 TCP      10.115.68.194:22446 <->     47.254.149.1:80          5        5      563       555
2022-04-20 09:52:05.802     0.002 UDP       185.64.40.2:46178 <->        8.8.4.4:53            1        1      106        90
2022-04-20 09:53:34.707     5.148 TCP       185.64.41.74:59894 <->   104.96.139.136:443         4        4      288       809
2022-04-20 09:48:22.864     0.036 UDP       185.64.40.1:10256 <->   205.251.192.207:53          1        1       82        93
2022-04-20 09:51:36.807     0.000 ICMP    185.64.40.253:0     <->   139.224.193.127:0.0         0        1        0       143
2022-04-20 09:50:38.914     2.081 TCP       185.64.40.27:61937 <->      20.42.65.89:443          9       11     7269      2118
2022-04-20 09:51:12.850     0.021 UDP       10.115.104.1:41775 <->         8.8.8.8:53            1        1      108        78
2022-04-20 09:48:44.488     0.436 TCP   2a03:11..9b:7e05.52811 <-> 2606:47..12:20c0.443          34       20    27273      2617
2022-04-20 09:49:57.282    50.587 TCP       10.115.5.43:50975 <->   108.177.126.109:993        906      637   570715     51667
2022-04-20 09:52:47.886    33.983 TCP       185.64.40.49:50502 <->   108.177.126.109:993        11        2      770       171
2022-04-20 09:48:32.899     0.000 ICMP    185.64.40.253:0     <->    188.166.69.73:0.0          0        1        0       106
2022-04-20 09:53:02.865     0.000 ICMP      185.64.40.1:0     <->    23.73.134.168:0.0          0        1        0        82
2022-04-20 09:48:23.811     0.143 UDP       10.115.0.253:51585 <->   205.251.198.39:53          1        1       84        95
2022-04-20 09:48:19.588   118.367 TCP       185.64.40.101:51538 <->    188.114.96.8:443         38       28    23414      4120     4
2022-04-20 09:51:55.894     0.035 UDP       185.64.41.73:53019 <->    172.224.37.11:443          0       11        0      4429     1
2022-04-20 09:49:36.734   245.209 TCP     10.115.245.225:44094 <->    142.251.36.78:443         11        9     6197      1219     3
Summary: total flows: 51, total bytes: 726043, total packets: 1829, avg bps: 14802, avg pps: 4, avg bpp: 396
Time window: 2022-04-20 09:46:39 - 2022-04-20 09:54:59
Total flows processed: 13546, Blocks skipped: 0, Bytes read: 1048520
Sys: 0.018s flows/second: 745022.5   Wall: 0.014s flows/second: 944630.4
root@collector:/usr/local/maxifi/www/nfe/data/nfdump/2022-04-20#
```

Maxifi
maximize your wi-fi network

Statistika nuda je, ale …

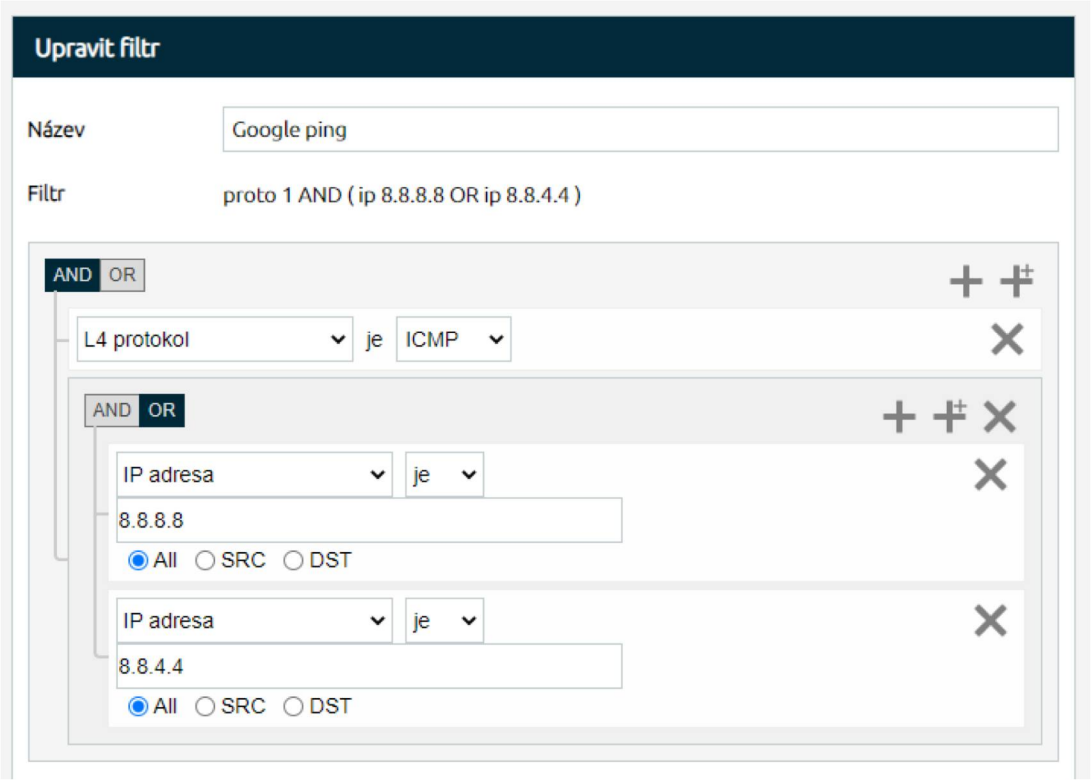
- Získání lepšího přehledu o dění na síti
- Datové objemy per IP (příjem, odesílání)
- Objem komunikace s jednotlivými sítěmi (AS)
- Interpretace komunikace dle státu apod.
- Skladba provozu (porty, počty flow)



Maxifi
maximize your wi-fi network

Filtry – nehledejme jehlu v kupce sena

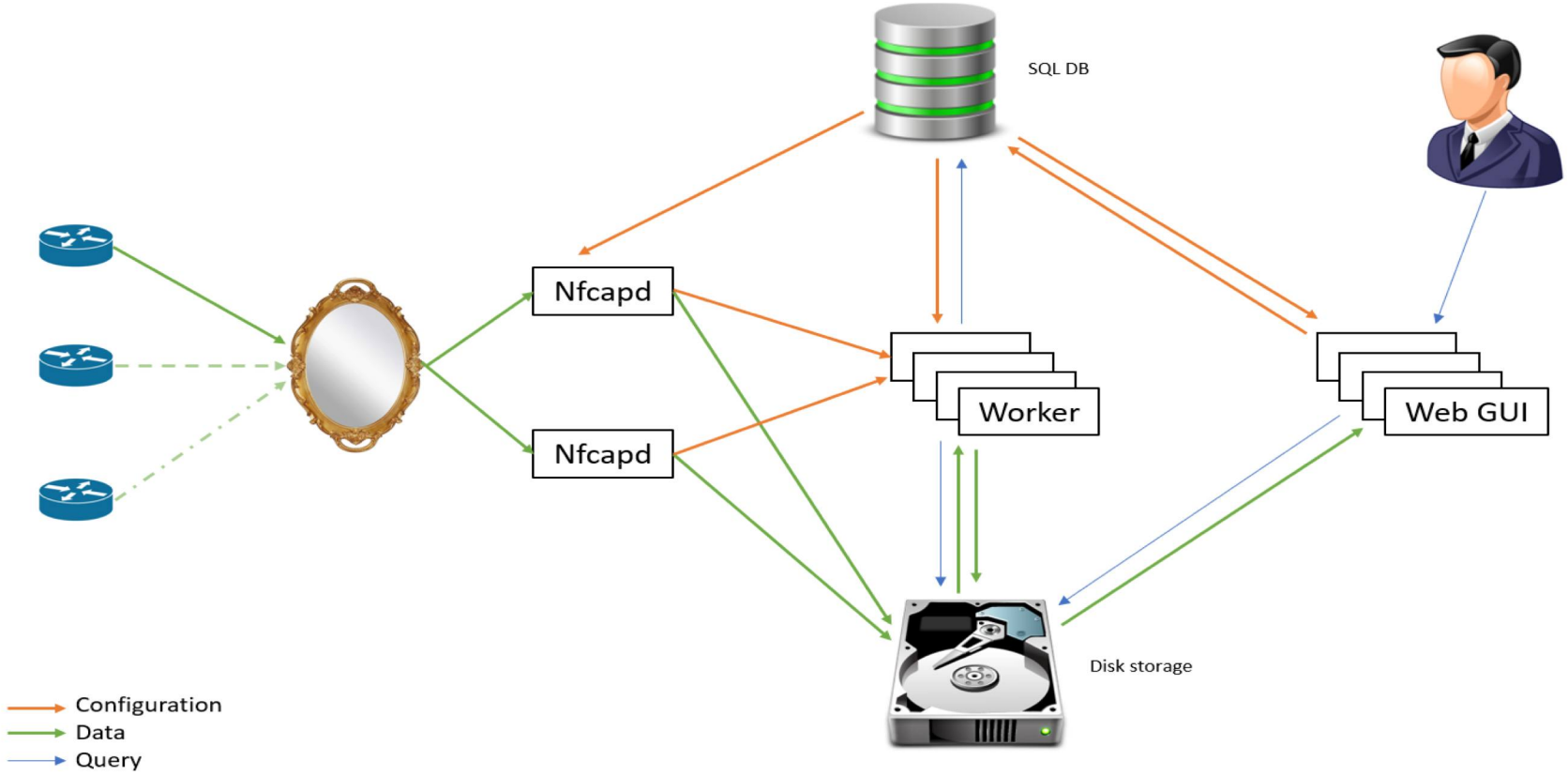
- Jednoduché grafické rozhraní pro nastavení filtrů
- Kontrola platnosti dat
- Bez omezení oproti CLI
- Možnosti ukládání, importu / exportu filtrů



Maxifi
maximize your wi-fi network

Zdroje dat – rozděl a panuj

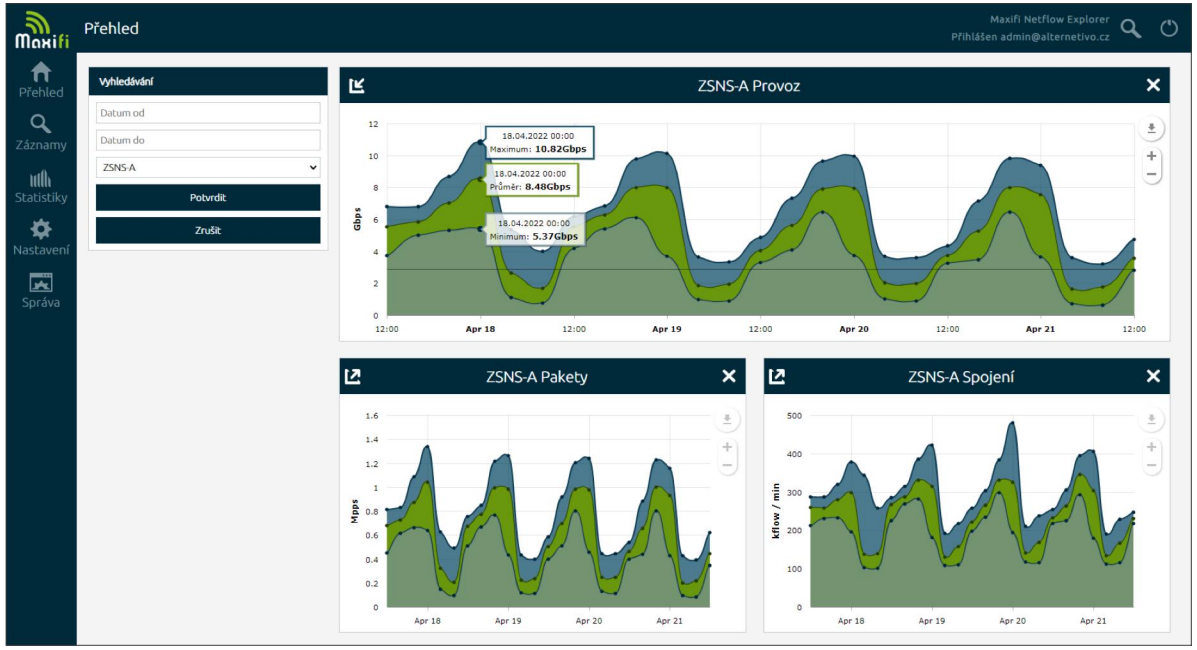
- Možnost filtrování, zpracování a korekce dat



Maxifi
maximize your wi-fi network

Proč Maxifi NFE ?

- Cenově atraktivní přesto robustní řešení pro sběr a interpretaci NetFlow dat
- Neřešíme jen NetFlow kolektor, řešíme NetFlow s ohledem na design celého jádra sítě ISP
- Stavíme na 25+ letech zkušeností z designu sítí pro ISP i operátory
- Cloud i OnPrem varianta nasazení
- Navrženo i podporováno v CZ pro CZ (/SK)
- Jednoduchost & komplexnost



A to je vše, děkujeme …