Návrh
řešení DR projektu
pro RETE internet s.r.o

Ověření možnosti nasazení Fortigate a Flowmon kolektoru pro řešení projektu DR a monitoring ISP sítě lokální velikosti

RETE internet s.r.o.

Poskytování připojení k internetu
především na vlastní optické síti

GraphTech spol. s r.o.

Řešení DR projektů

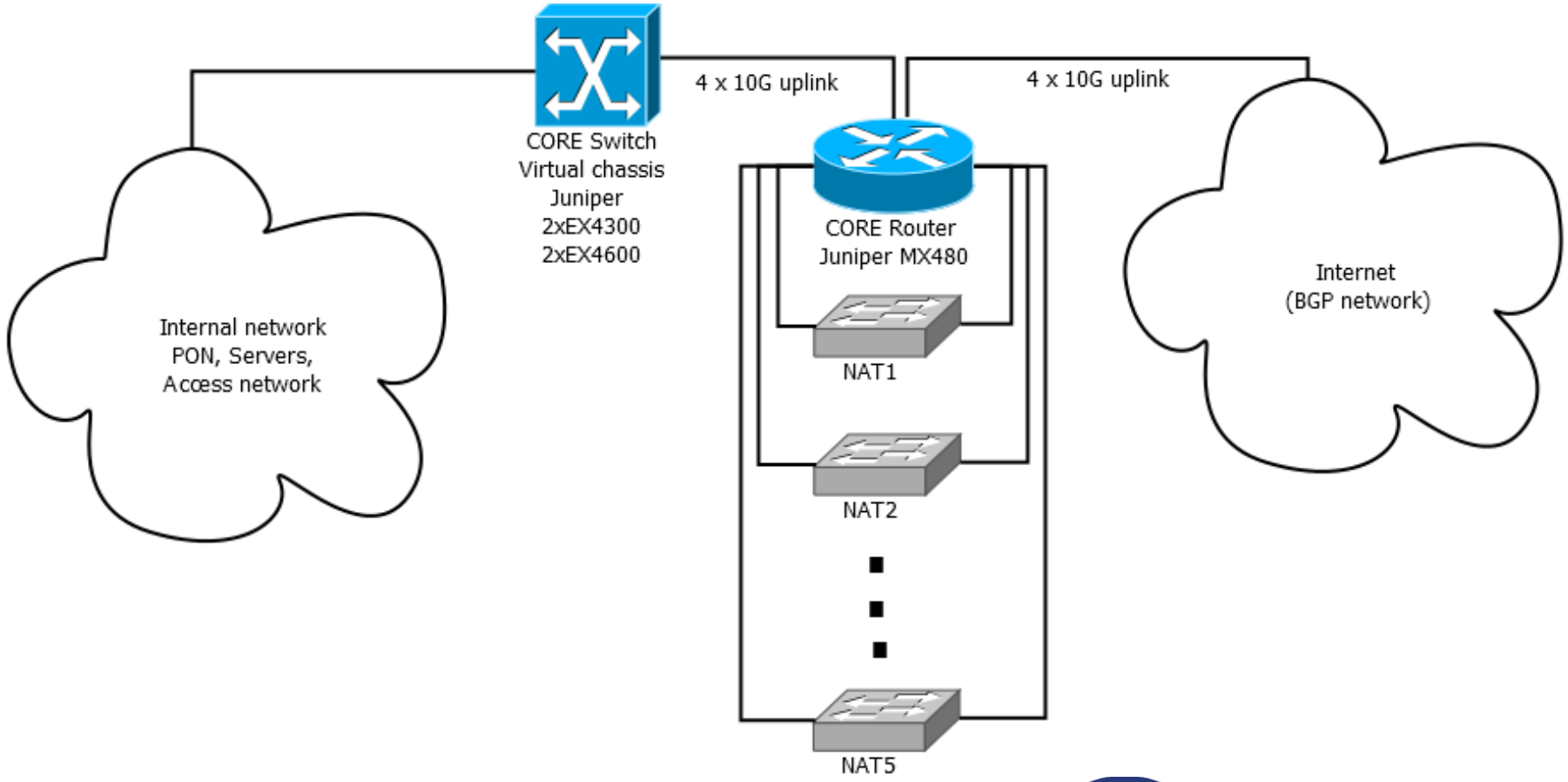
FORTINET®

Progress® | Flowmon

rete internet

GraphTech

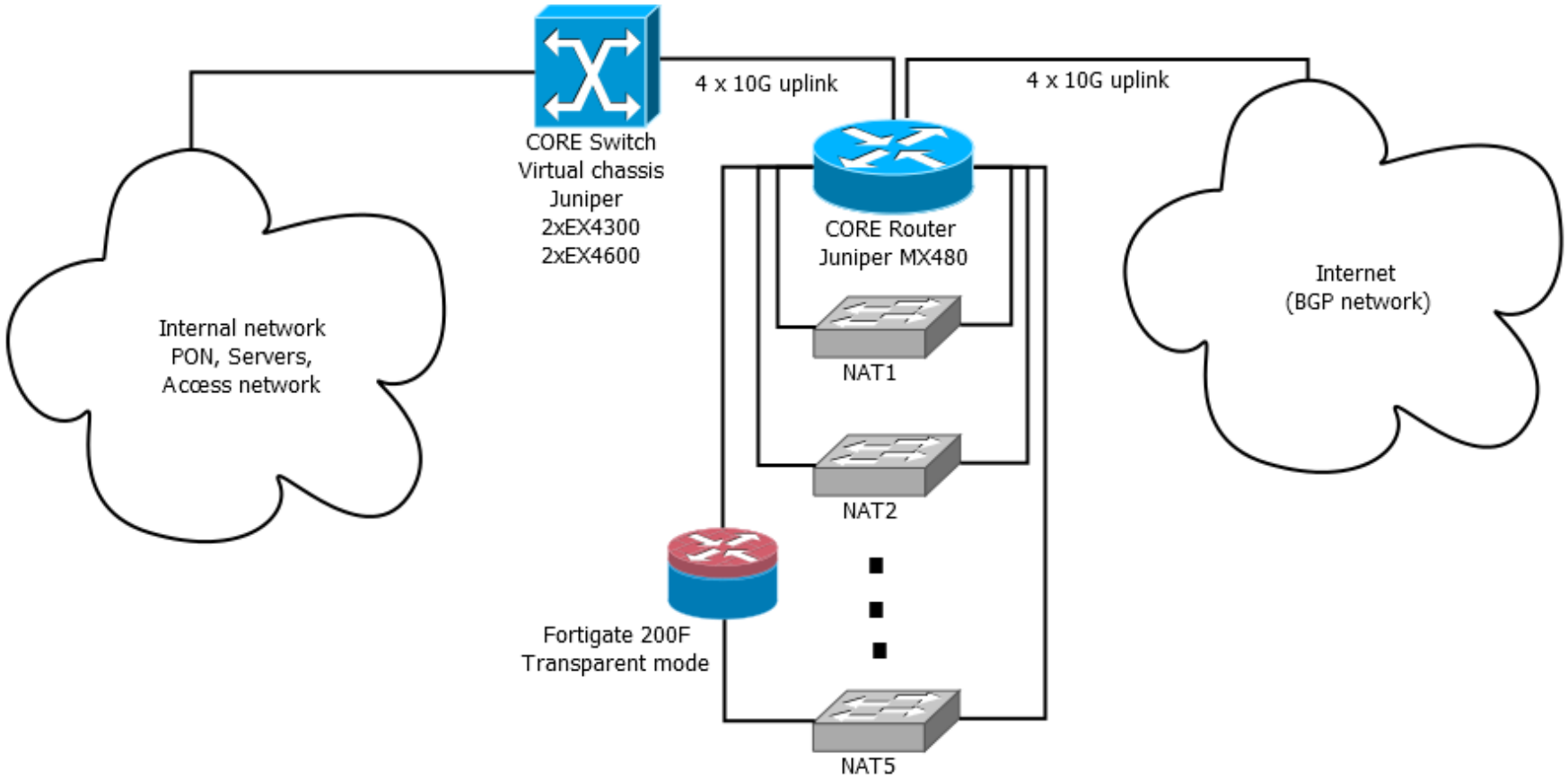
Topologie sítě v Roudnici n.L.



rete internet

GraphTech

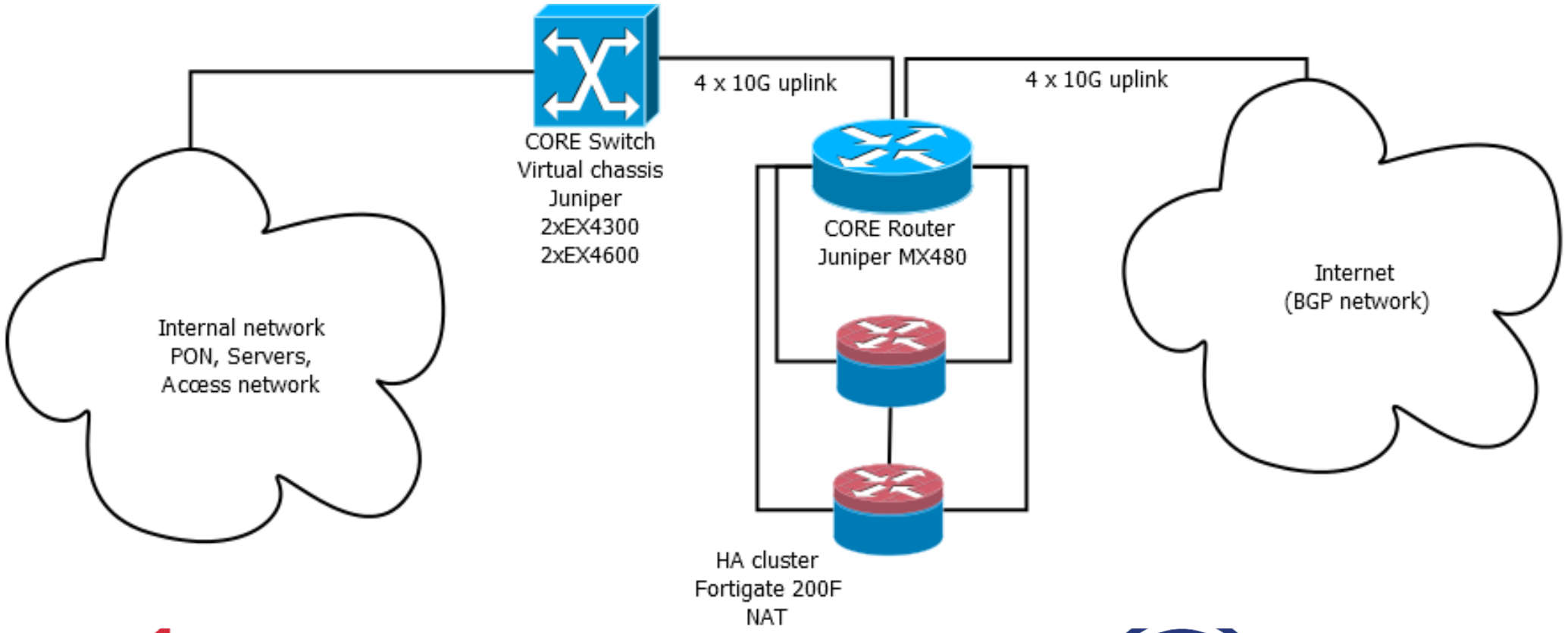
Testovací zapojení Fortigate 200F



rete internet

GraphTech

Finální zapojení Fortigate 200F



rete internet

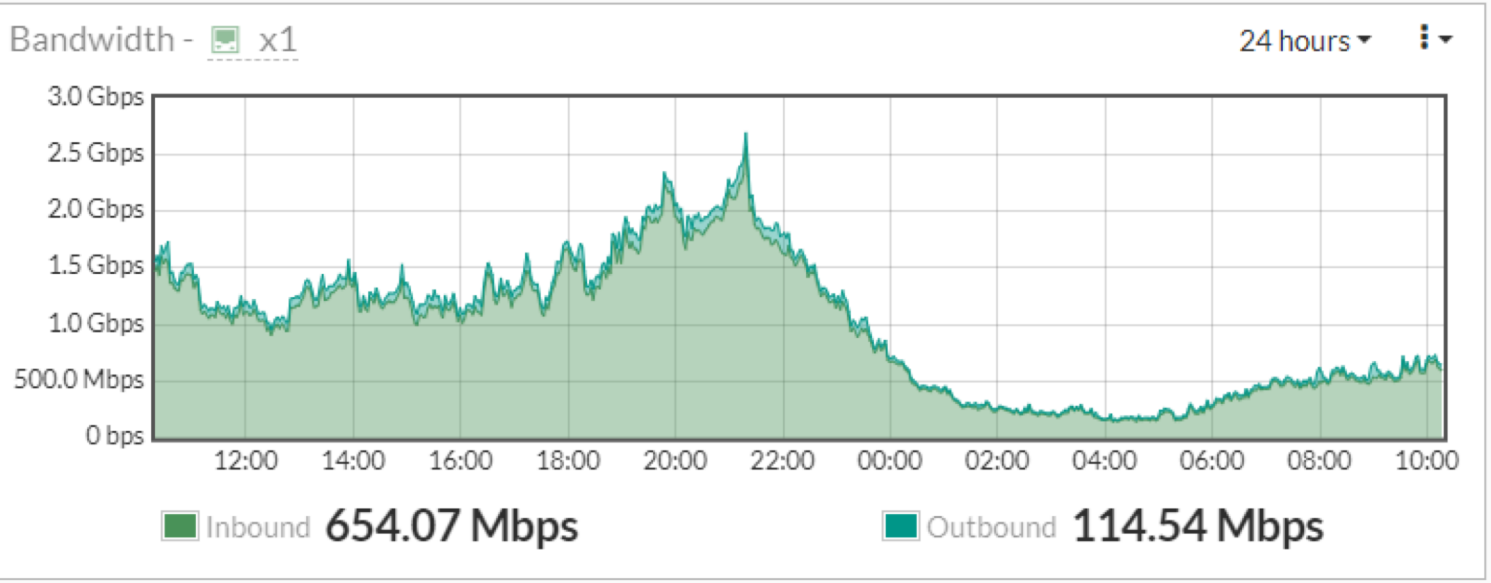
GraphTech

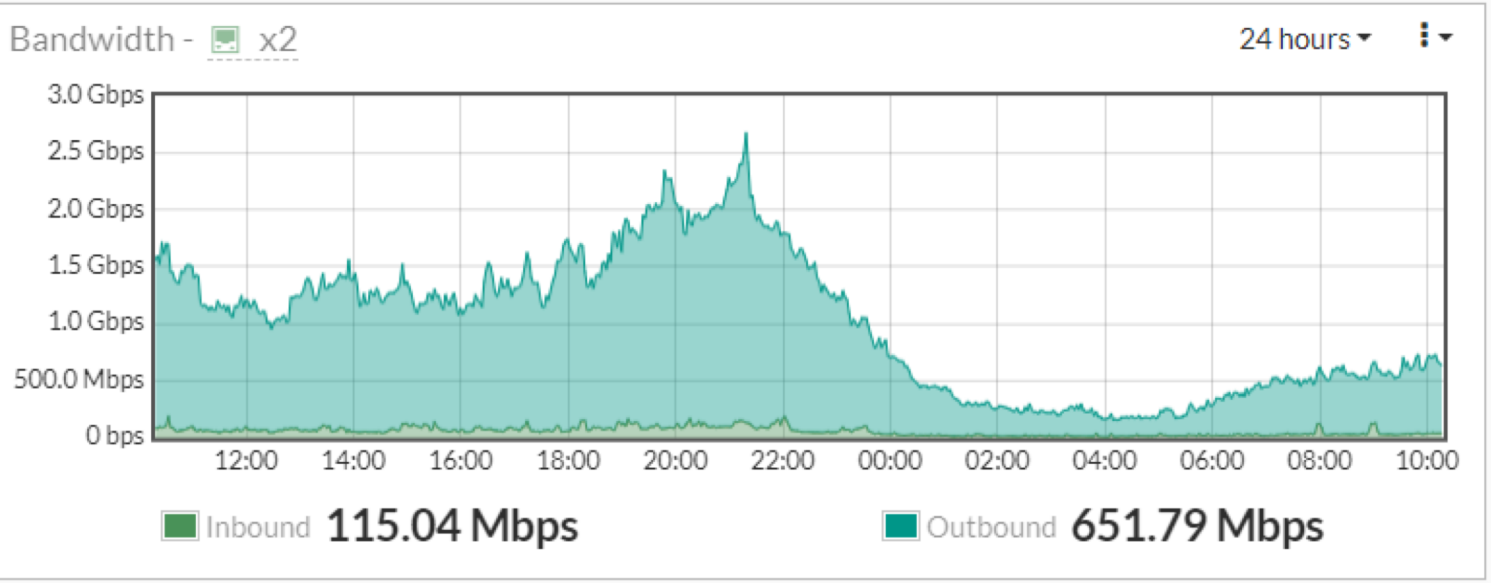
Konfigurace Fortigate 200F

- Odběr NetFlow na portu SFP+ 10Gbps
- Firewall pravidla
- Transparentní mód
- Kontrola antivirem
- Kontrola aplikací
- SSL inspekce
- Ochrana před DDoS
- Traffic shaping

rete internet

GraphTech





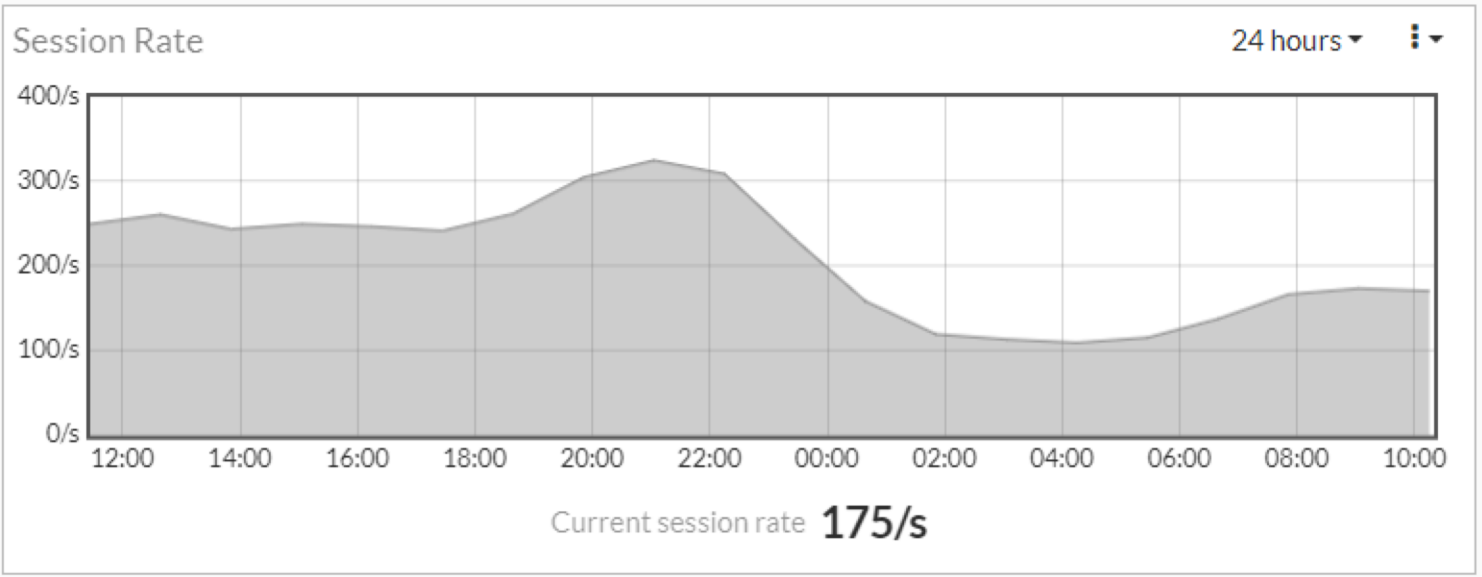
Graf provozu při testu

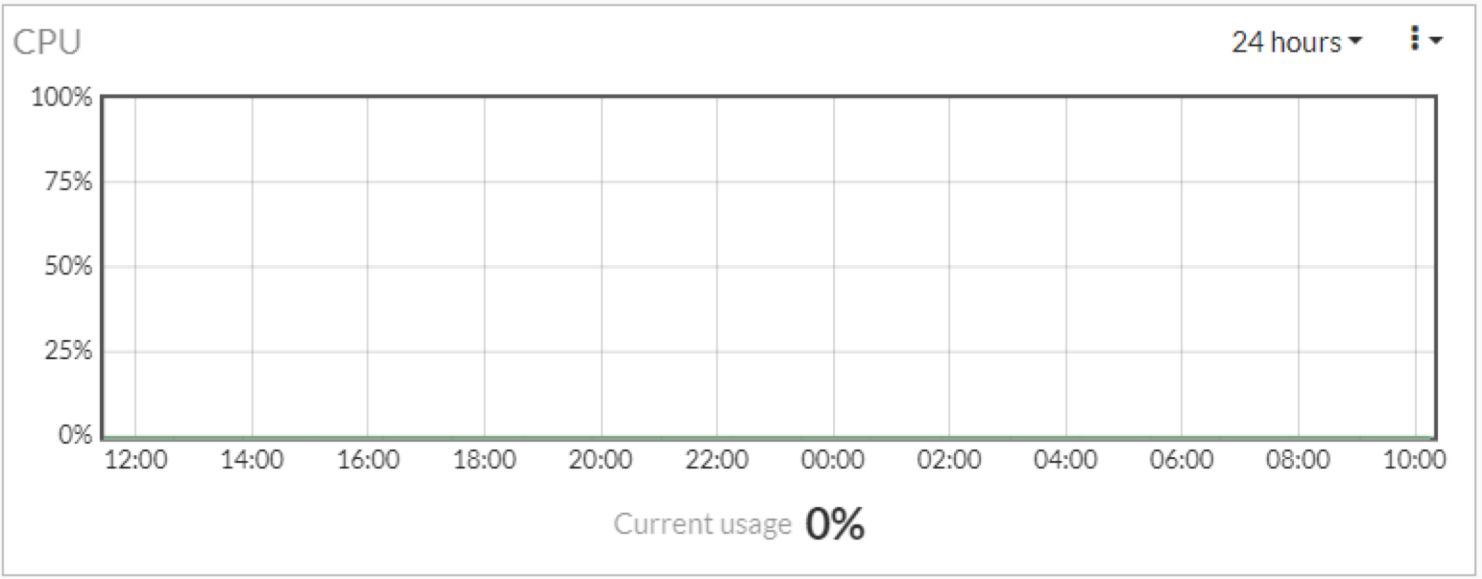
Kumulativní provoz
Maximum Input
2,7Gbps

Maximum Output
2,7Gbps

rete internet

GraphTech





Graf vytížení CPU

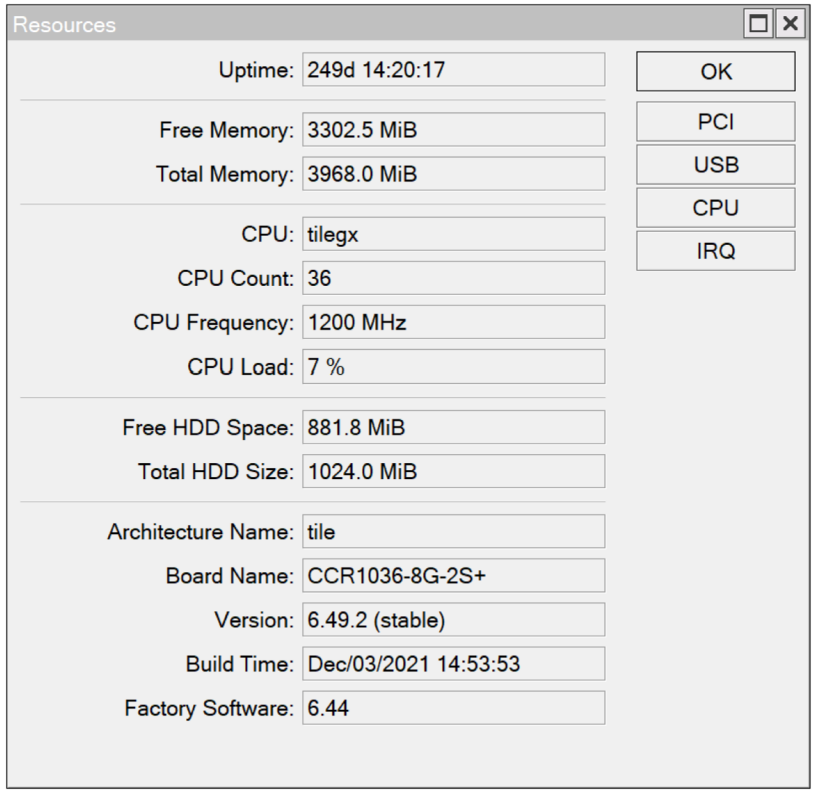
Maximum Session
310/s

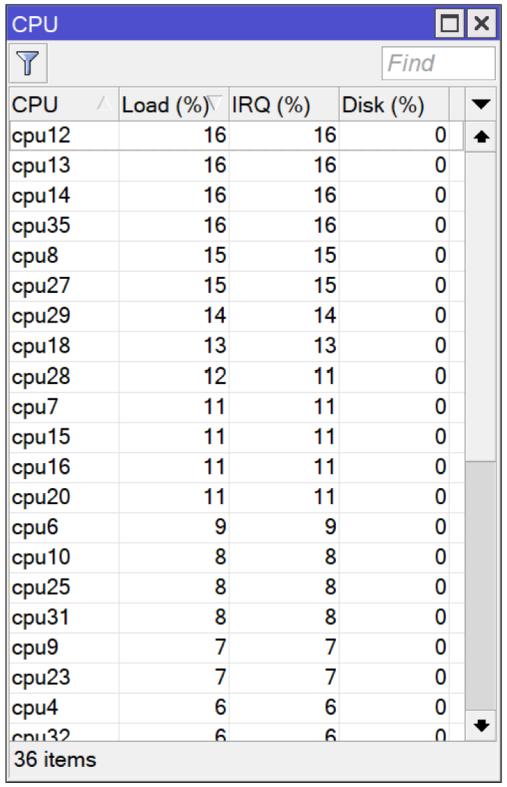
Maximum CPU
0,5%

rete internet

GraphTech

sfp-sfpplus1	Ethernet	1500	1580	78.3 Mbps	1874.3 Mbps	61 497	175 698	78.3 Mbps
sfp-sfpplus2	Ethernet	1500	1580	1869.1 Mbps	72.7 Mbps	170 233	55 950	1869.1 Mbps





Graf vytížení CPU Mikrotik

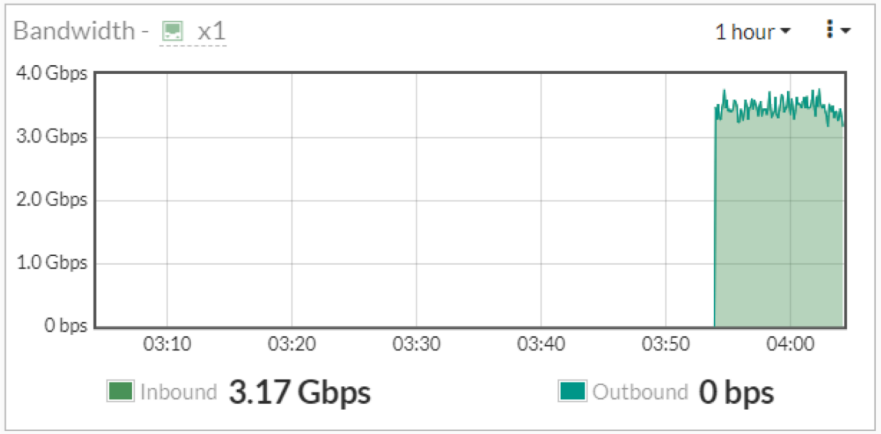
AVG 7%

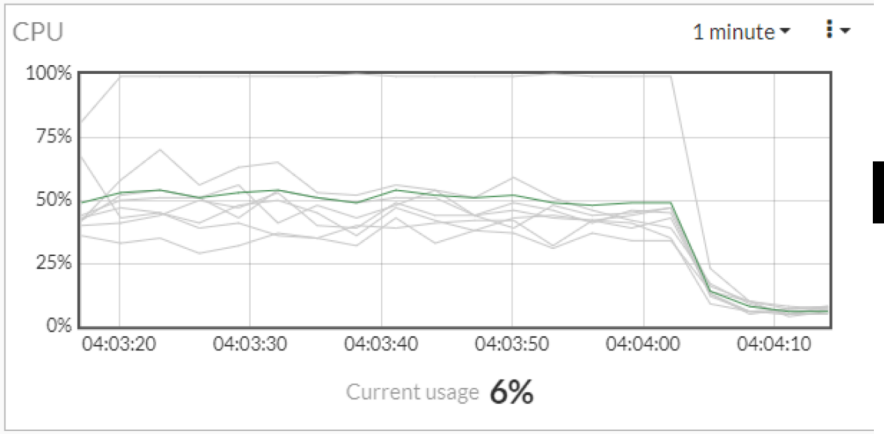
MAX core CPU 16%

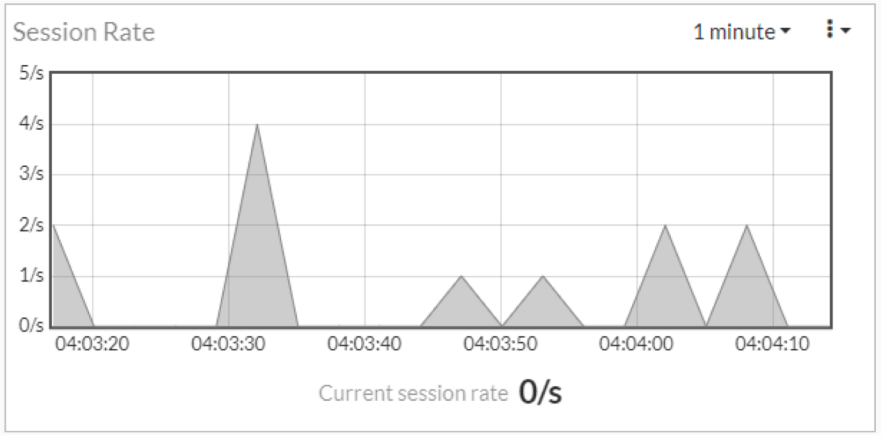
rete internet

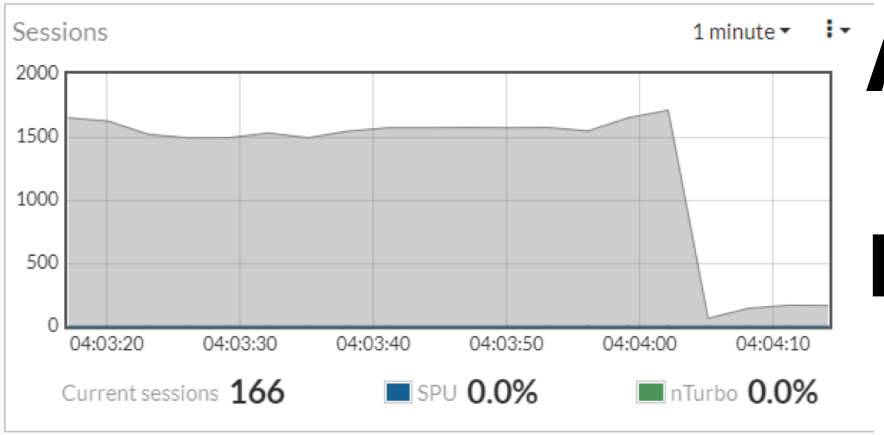
GraphTech

Vytížení CPU, nelegitimní provoz









Maximum Input
3,2Gbps

AVG CPU
50%
Max core CPU
100%

rete internet

GraphTech

Fortigate jako zdroj NetFlow

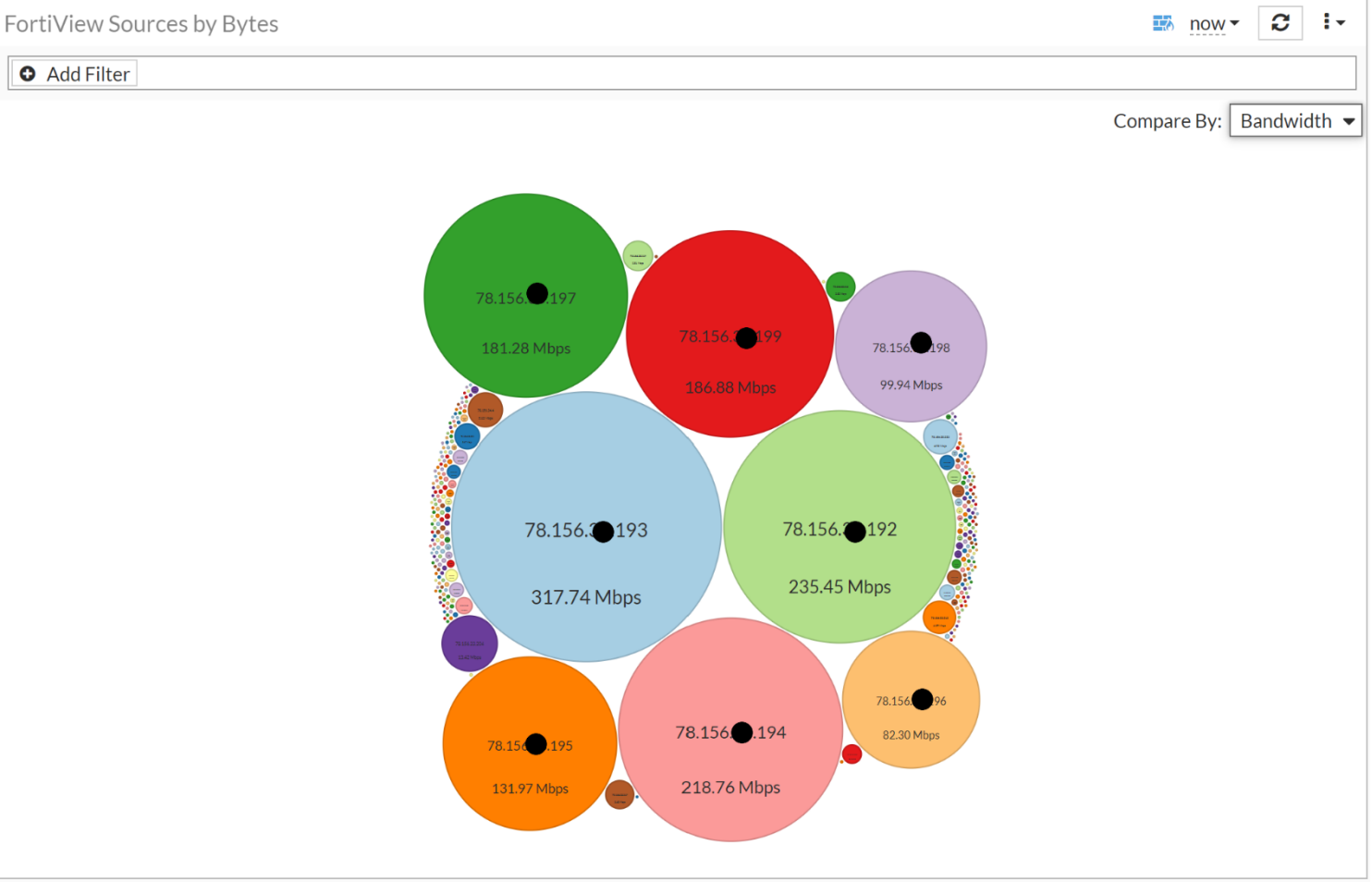
- Plný odběr hlaviček paketů
- Hardwarová podpora
- Konfigurace na více portů
- Plně vyhovuje potřebám DR

rete internet

GraphTech

Monitoring provozu a vyhledání problému

- DDoS - online FortiGate
- Traffic shaping - online Fortigate
- Antivir - online Fortigate
- Firewall - online Fortigate
- Application control - online Fortigate
- SLA - Flowmon kolektor
- DR report - Flowmon kolektor
- Anomální chování – Flowmon kolektor

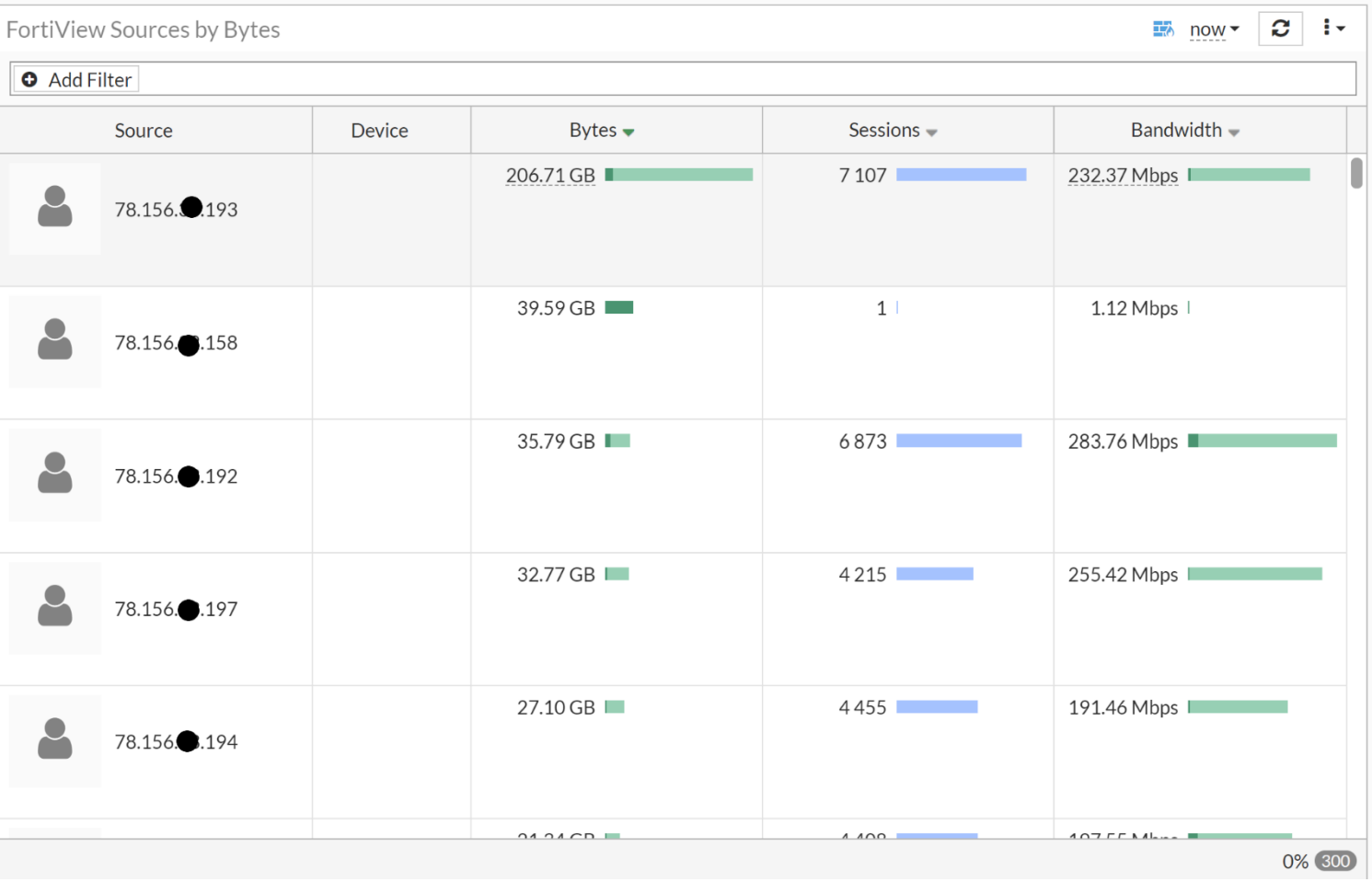


FG přehled provozu

Aktuální provoz [Mbps] na IP adresách

rete internet

GraphTech



FG přehled provozu

Aktuální provoz na IP adresách 78.156.xx.193

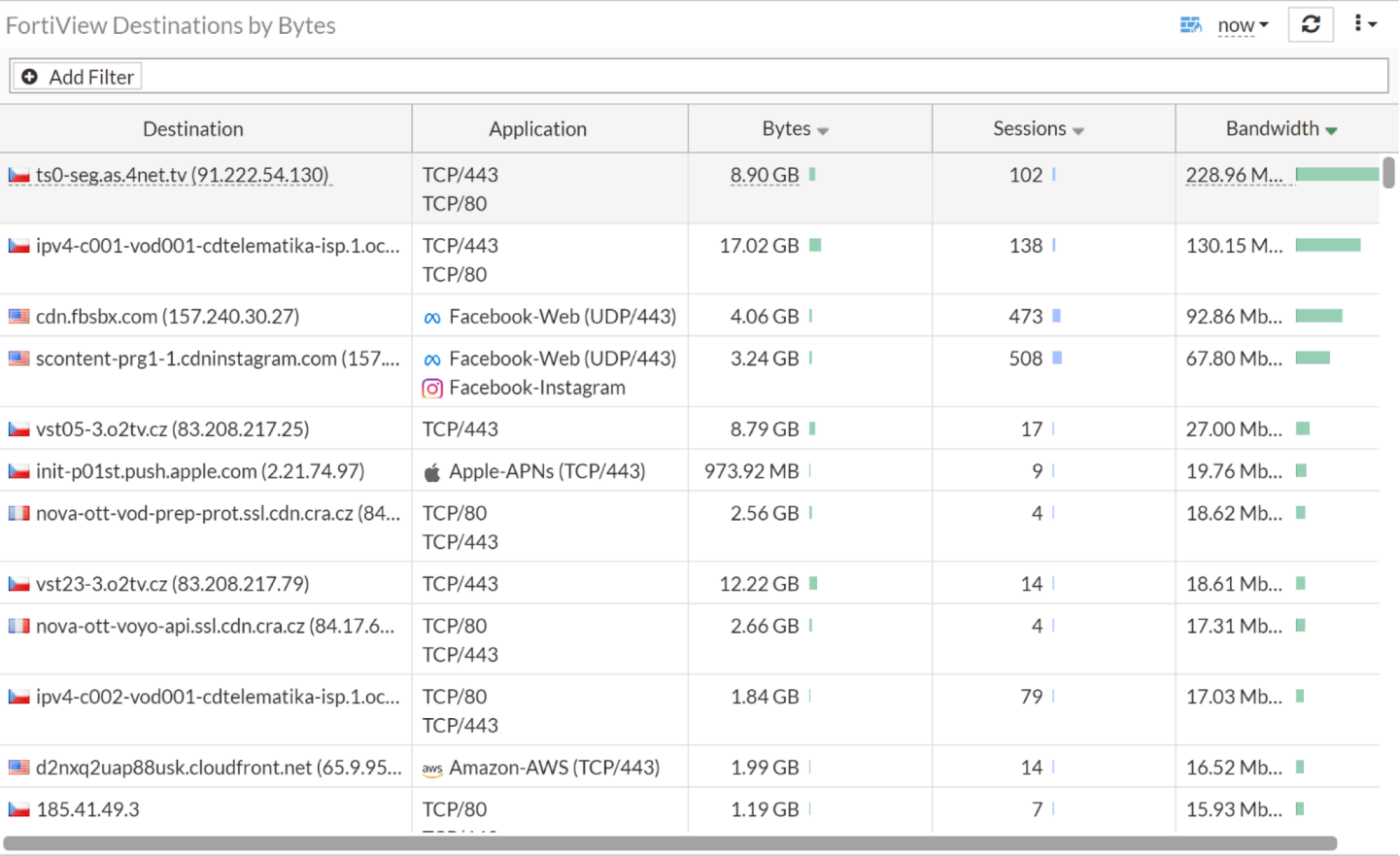
232 Mbps

7107 Sessions

206 GB

rete internet

GraphTech

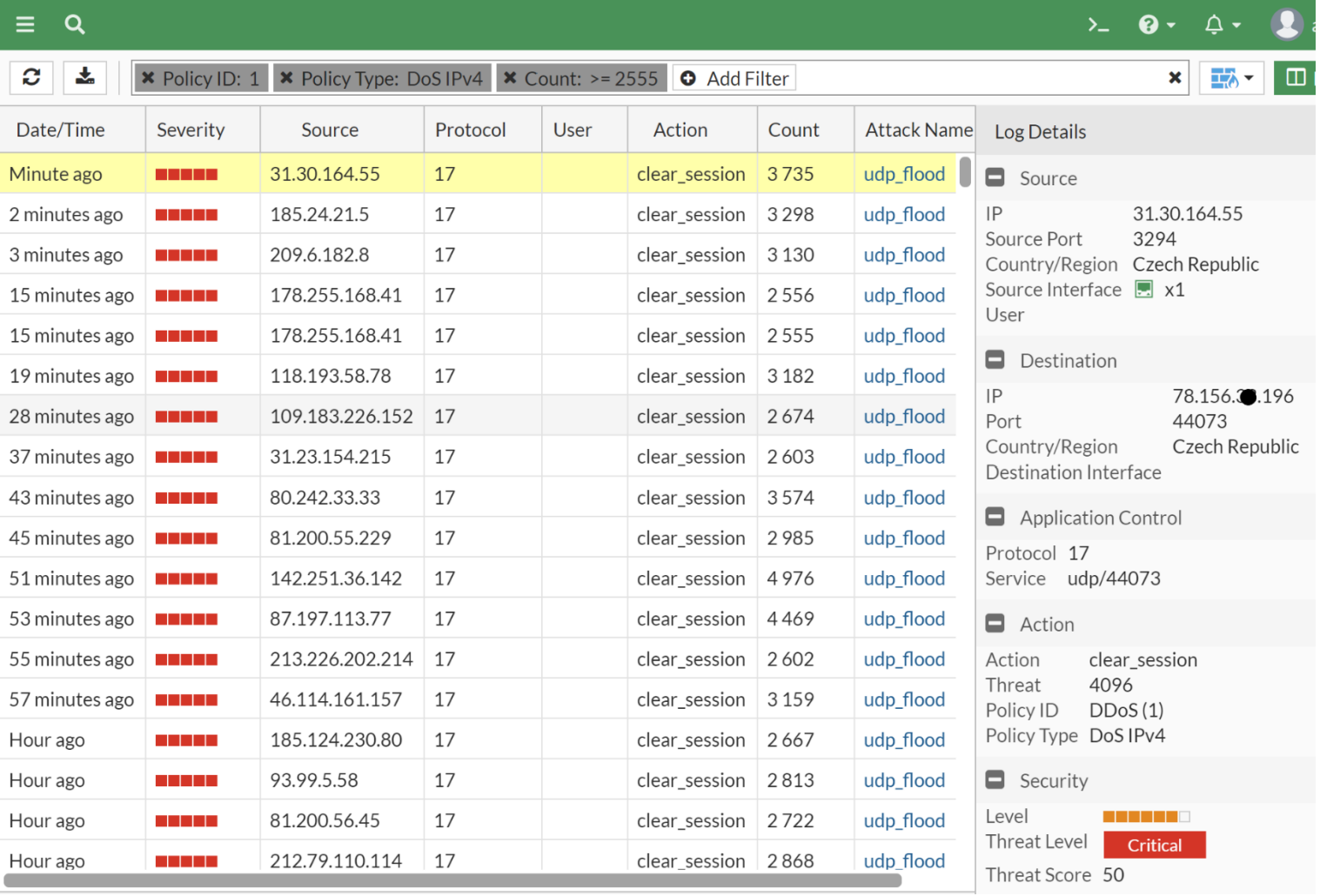


FG přehled provozu

Aktuální provoz dle destination ts0-seg.as.4net.tv sessions 102 rychlost 228Mbps

rete internet

GraphTech

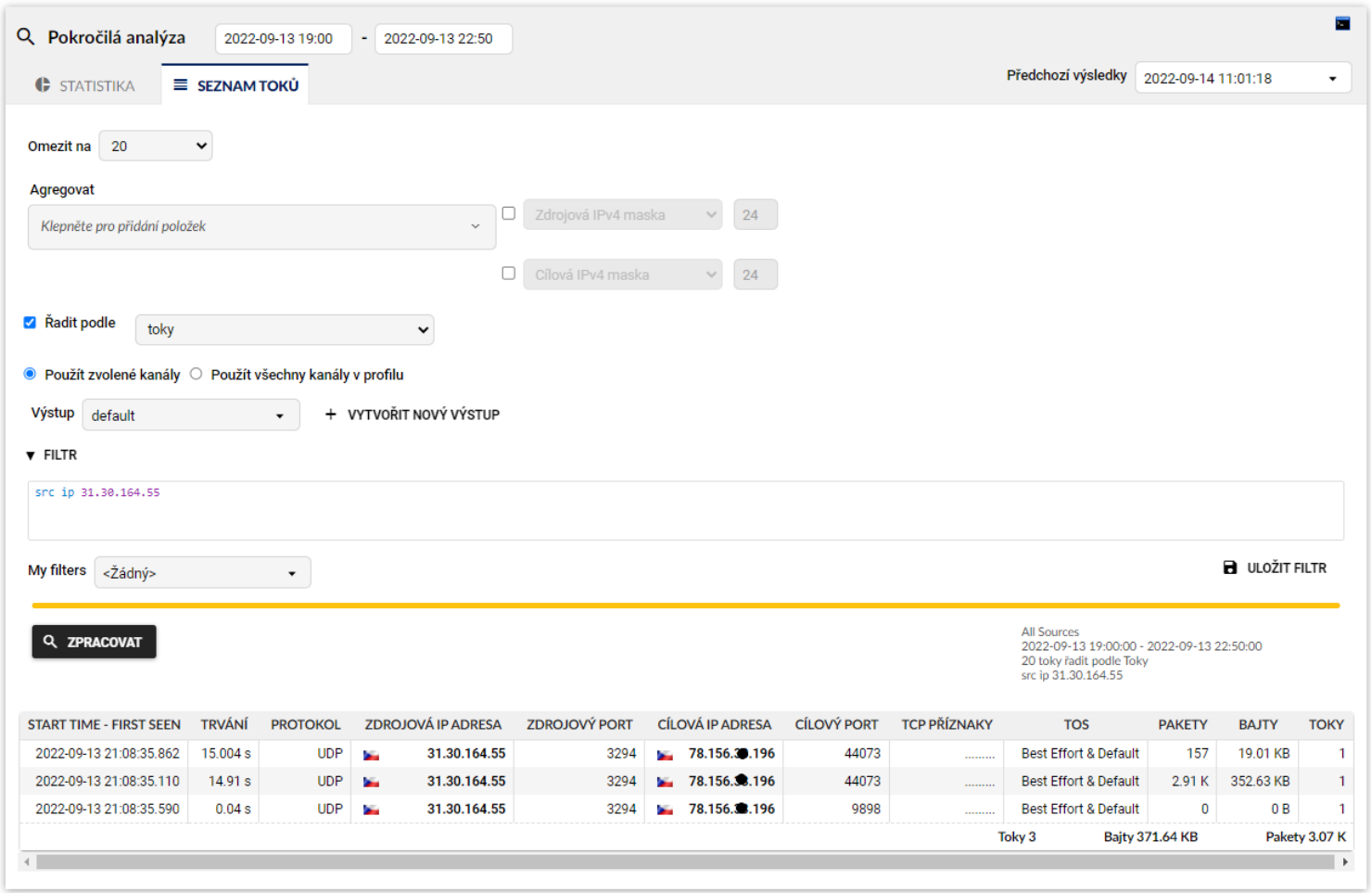


FG přehled provozu

Seznam DDoS incidentů
src 31.30.164.55
Dst 78.156.xx.196
src port udp/3294
dst port udp/44073
attack udp_flood

rete internet

GraphTech



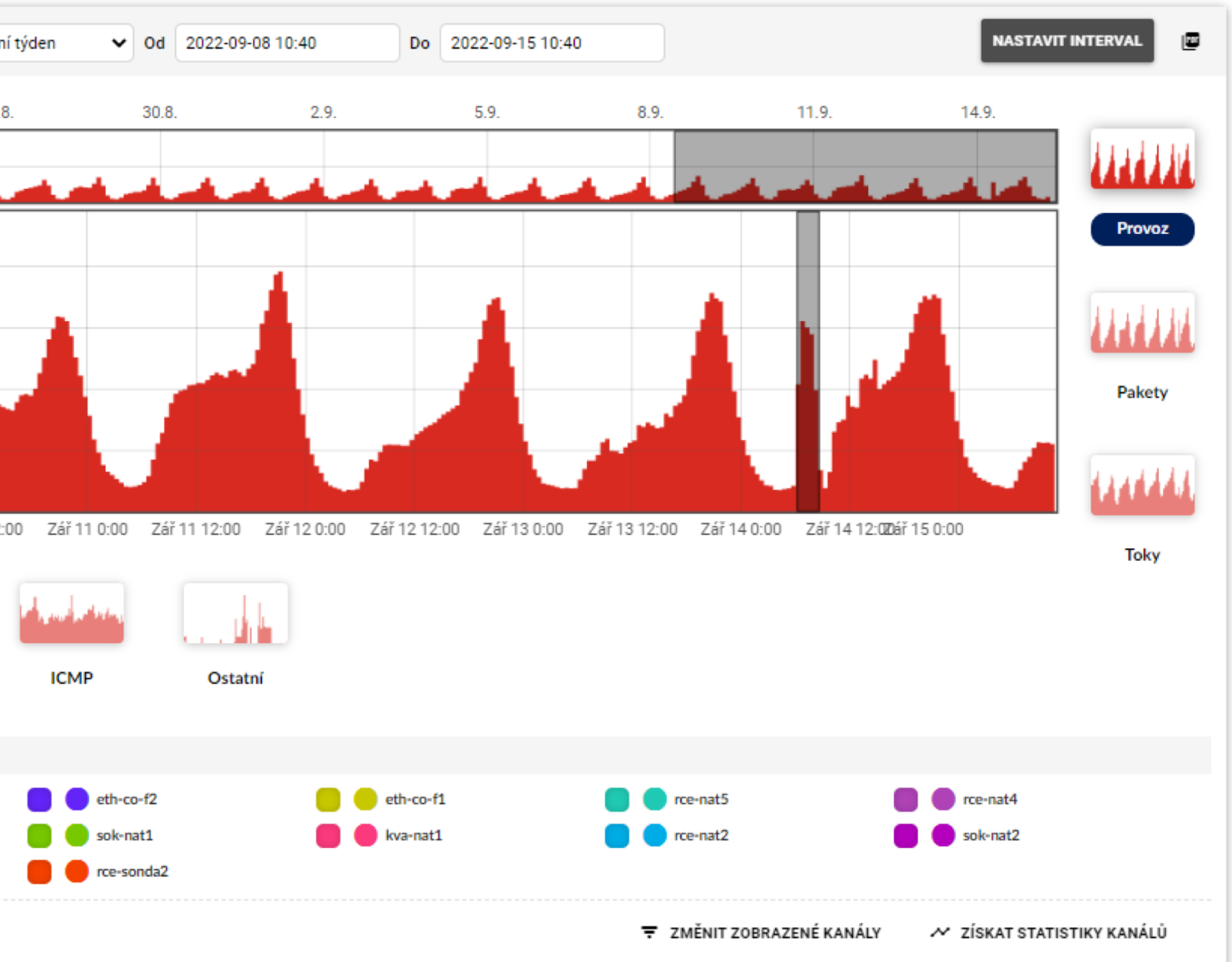
Flowmon kolektor

Kontrola funkce DDoS ochrany na Flowmon kolektoru

Počet paketů: před FG 2910 za FG 157

reteinternet

GraphTech



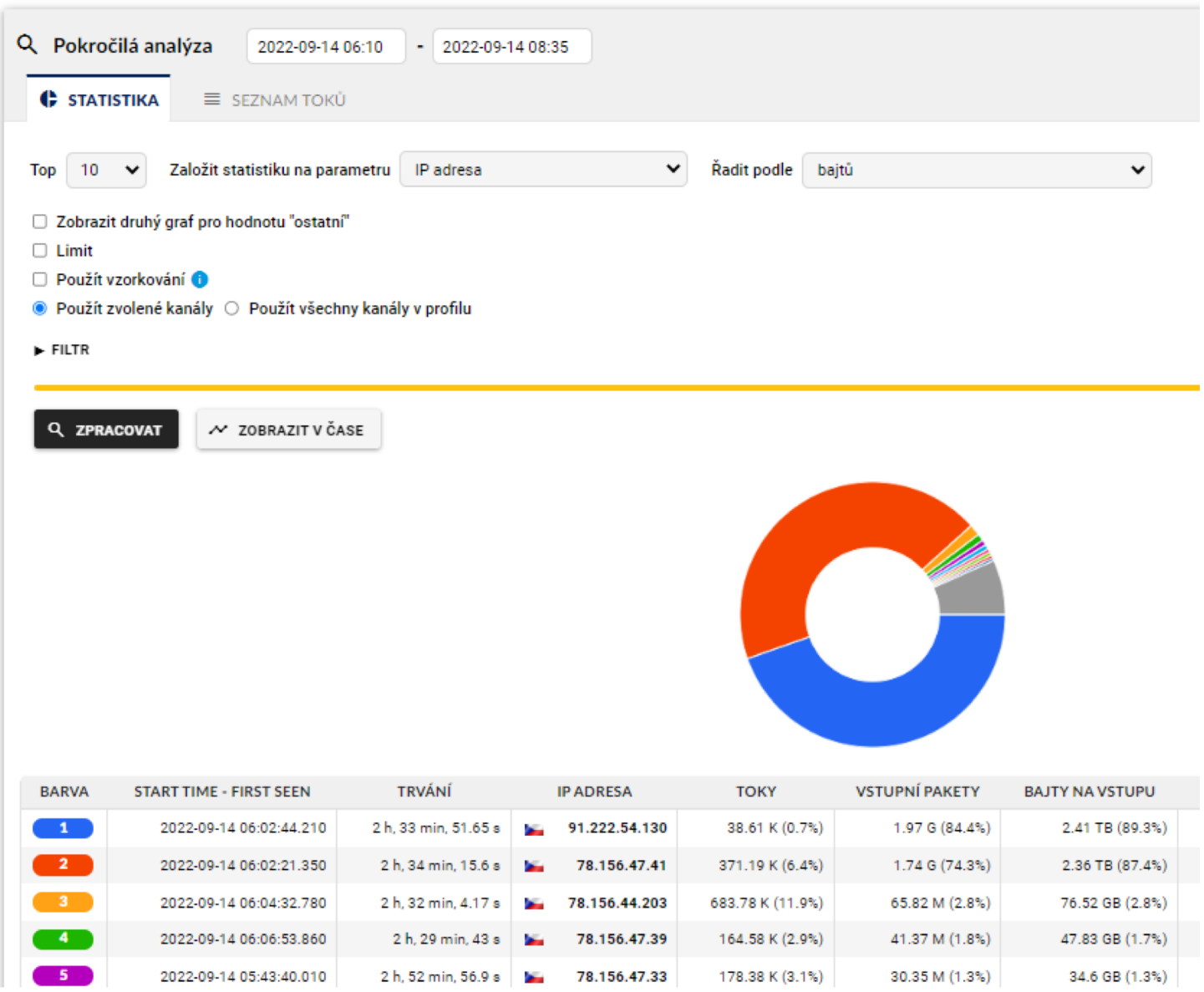
Flow kolektor

Běžná volumetrická kontrola provozu 7. dní zpět

Nalezení nestandartního provozu

rete internet

GraphTech



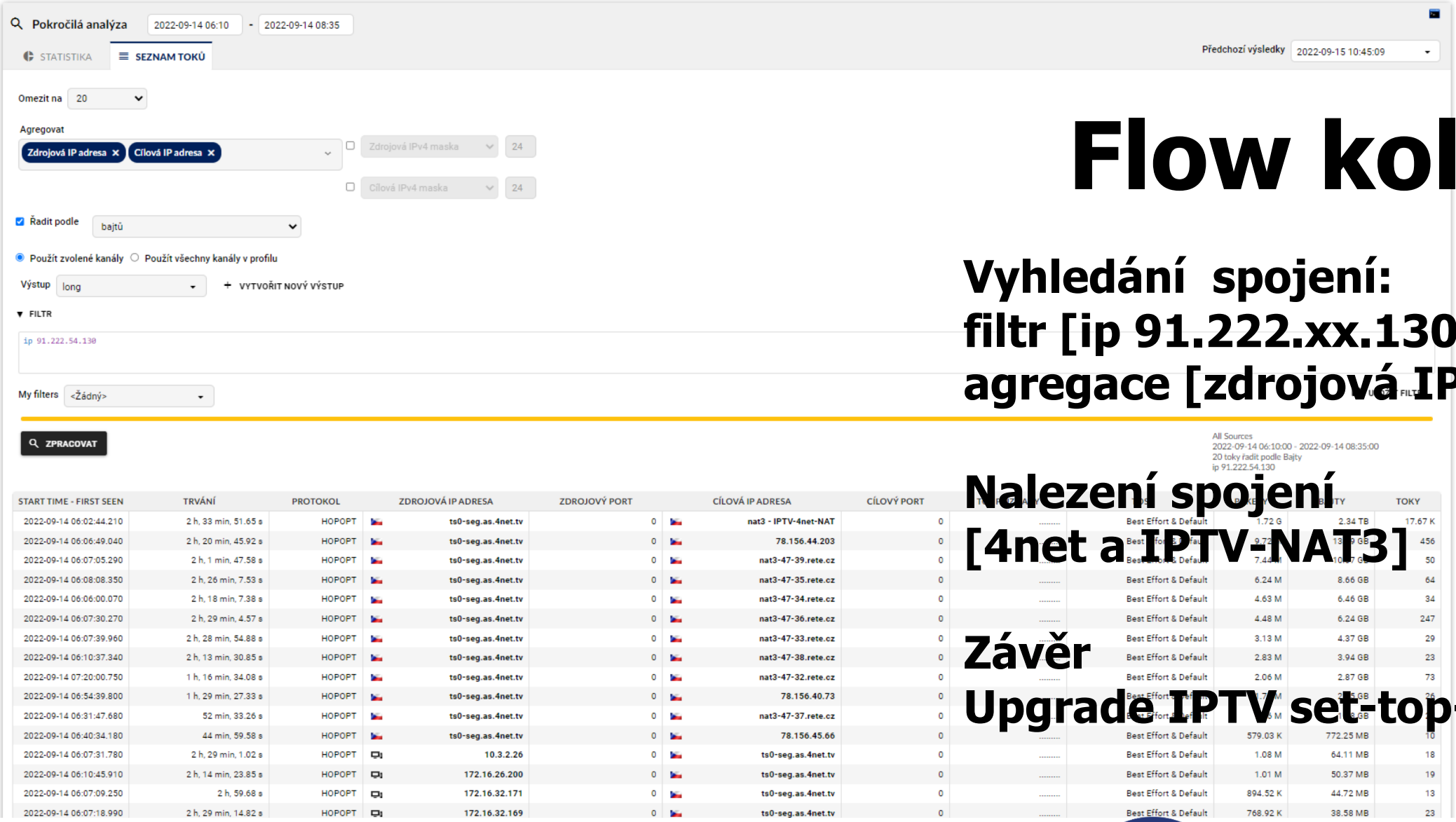
Flow kolektor

Vyhledání příčiny nestandartního provozu pomocí statistiky

Top IP 91.222.xx.130 provoz 2,3Gbps

rete internet

GraphTech



START TIME - FIRST SEEN	TRVÁNÍ	PROTOKOL	ZDROJOVÁ IP ADRESA	ZDROJOVÝ PORT	CÍLOVÁ IP ADRESA	CÍLOVÝ PORT	TOS	BAJTY	TOKY
2022-09-14 06:02:44.210	2 h, 33 min, 51.65 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3 - IPTV-4net-NAT	0	Best Effort & Default	2.34 TB	17.67 K
2022-09-14 06:06:49.040	2 h, 20 min, 45.92 s	HOPOPT	ts0-seg.as.4net.tv	0	78.156.44.203	0	Best Effort & Default	13.09 GB	456
2022-09-14 06:07:05.290	2 h, 1 min, 47.58 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-39.rete.cz	0	Best Effort & Default	7.44 M	50
2022-09-14 06:08:08.350	2 h, 26 min, 7.53 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-35.rete.cz	0	Best Effort & Default	6.24 M	64
2022-09-14 06:06:00.070	2 h, 18 min, 7.38 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-34.rete.cz	0	Best Effort & Default	4.63 M	34
2022-09-14 06:07:30.270	2 h, 29 min, 4.57 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-36.rete.cz	0	Best Effort & Default	4.48 M	247
2022-09-14 06:07:39.960	2 h, 28 min, 54.88 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-33.rete.cz	0	Best Effort & Default	3.13 M	29
2022-09-14 06:10:37.340	2 h, 13 min, 30.85 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-38.rete.cz	0	Best Effort & Default	2.83 M	23
2022-09-14 07:20:00.750	1 h, 16 min, 34.08 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-32.rete.cz	0	Best Effort & Default	2.06 M	73
2022-09-14 06:54:39.800	1 h, 29 min, 27.33 s	HOPOPT	ts0-seg.as.4net.tv	0	78.156.40.73	0	Best Effort & Default	1.79 M	16
2022-09-14 06:31:47.680	52 min, 33.26 s	HOPOPT	ts0-seg.as.4net.tv	0	nat3-47-37.rete.cz	0	Best Effort & Default	1.79 M	16
2022-09-14 06:40:34.180	44 min, 59.58 s	HOPOPT	ts0-seg.as.4net.tv	0	78.156.45.66	0	Best Effort & Default	579.03 K	772.25 MB 10
2022-09-14 06:07:31.780	2 h, 29 min, 1.02 s	HOPOPT	10.3.2.26	0	ts0-seg.as.4net.tv	0	Best Effort & Default	1.08 M	64.11 MB 18
2022-09-14 06:10:45.910	2 h, 14 min, 23.85 s	HOPOPT	172.16.26.200	0	ts0-seg.as.4net.tv	0	Best Effort & Default	1.01 M	50.37 MB 19
2022-09-14 06:07:09.250	2 h, 59.68 s	HOPOPT	172.16.32.171	0	ts0-seg.as.4net.tv	0	Best Effort & Default	894.52 K	44.72 MB 13
2022-09-14 06:07:18.990	2 h, 29 min, 14.82 s	HOPOPT	172.16.32.169	0	ts0-seg.as.4net.tv	0	Best Effort & Default	768.92 K	38.58 MB 23

Flow kolektor

Vyhledání spojení:
filtr [ip 91.222.xx.130]
agregace [zdrojová IP][cílová IP]

Nalezení spojení
[4net a IPTV-NAT3]

Závěr
Upgrade IPTV set-top-boxů

rete internet

GraphTech

Flowmon kolektor & Fortigate komplexní monitoring

- Online monitoring provozu
- Online řešení incidentů
- Online ochrana provozu
- Řešení SLA parametrů
- Dohledávání nestandartních událostí
- Plánování směrování provozu
- Predikce vývoje nárustu objemu provozu
- Podpora při řešení reklamací

rete internet

GraphTech

Flowmon kolektor & Fortigate komplexní DR řešení

- Fortigate transparentní mód
- Fortigate NAT mód
- Výstup z kolektoru vyhovuje standartu DR
- Možnost sběru NetFlow z jiných zařízení
- Výrobci podporovaný interface Flowmon a Fortinet

rete internet

GraphTech

Komplexní projekt

- Návrh technického řešení
- Vypracování žádosti o refundaci
- Realizace projektu
- Provozní podpora projektu
- Navštivte nás na stánku Fortinet

rete internet

GraphTech

Patrik Prešl

patrik.presl@rete.cz