

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



GraphTech

RETE internet s.r.o.

Poskytování připojení k internetu
především na vlastní optické síti

GraphTech spol. s r.o.

Řešení DR projektů

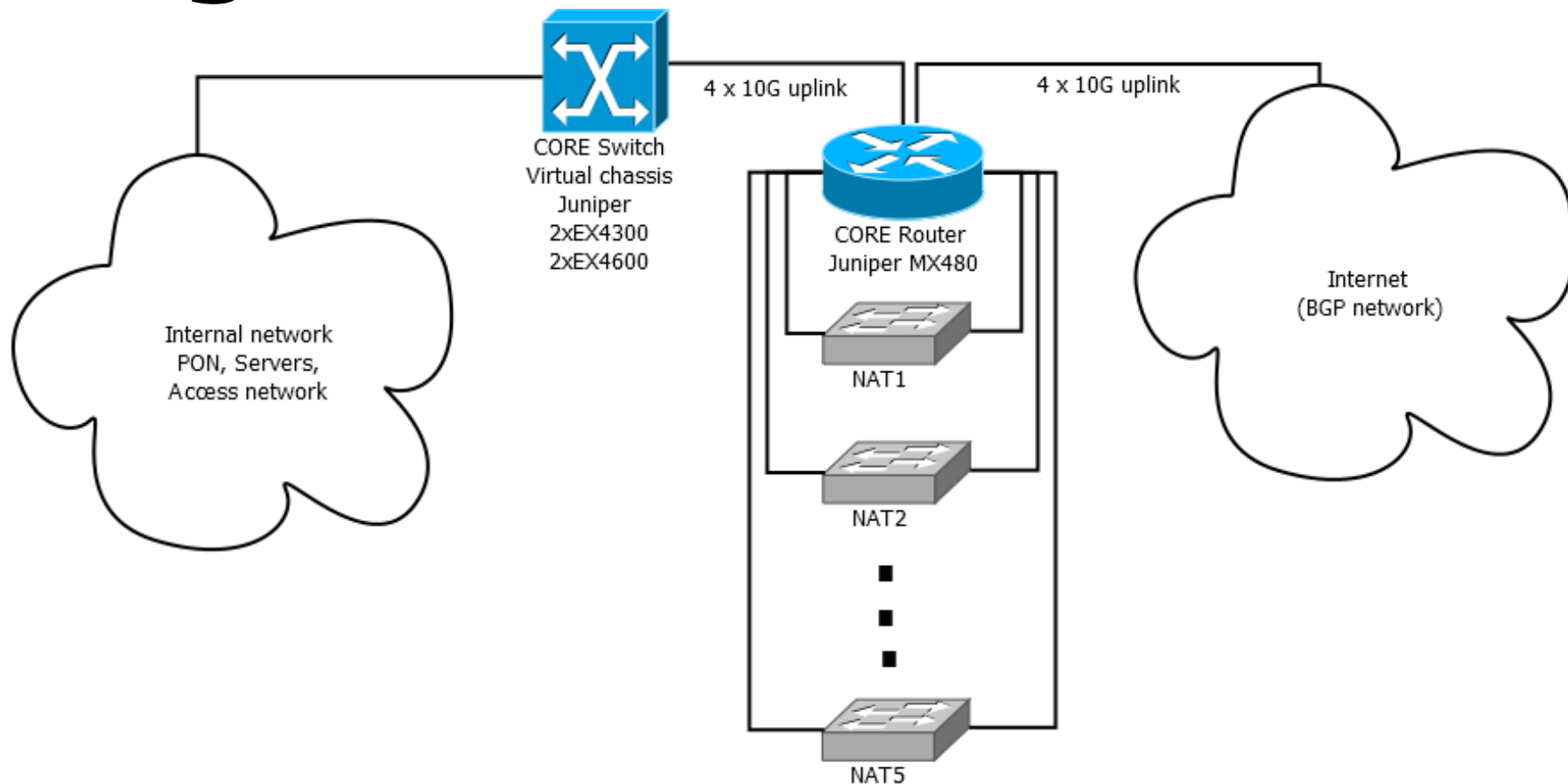
FORTINET®

 **Progress**® | **Flowmon**

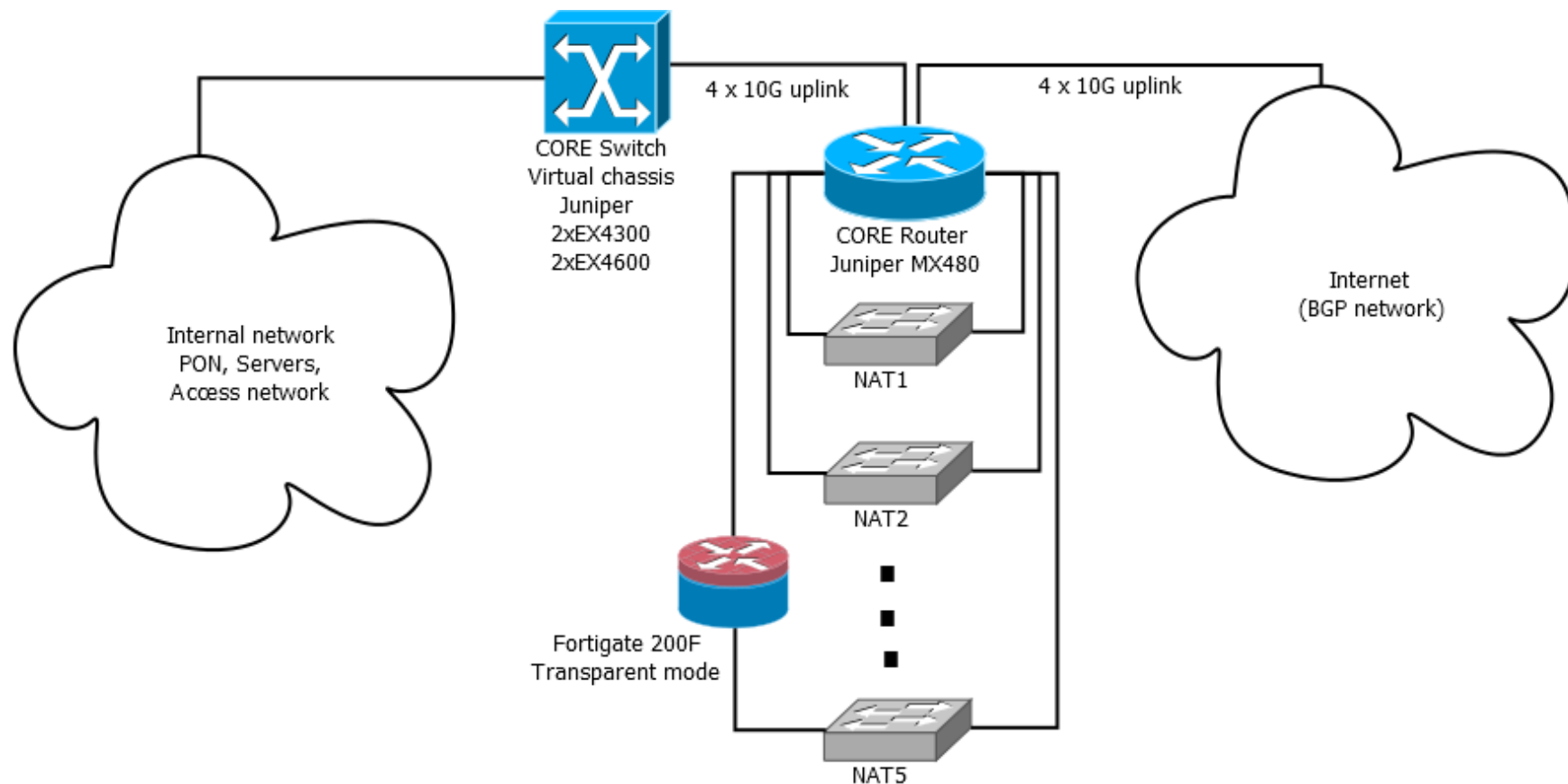
reteinternet

 **GraphTech**

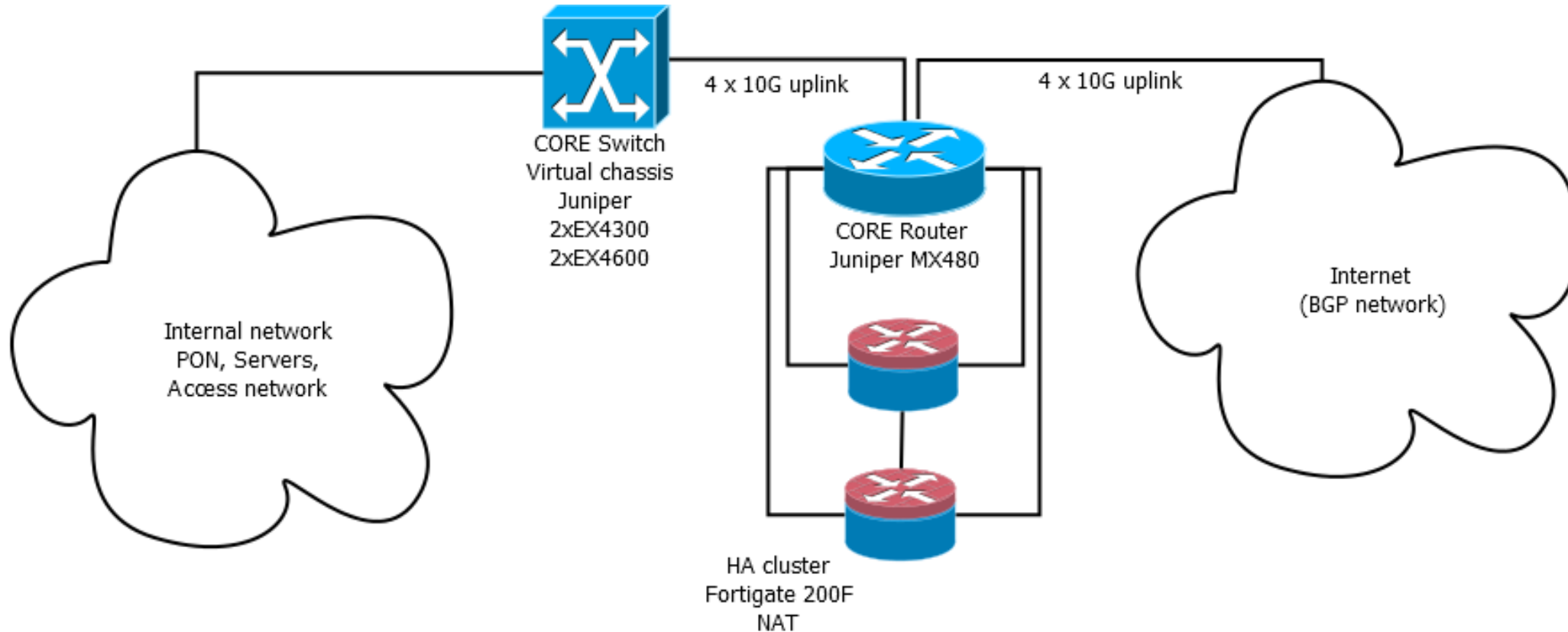
Topologie sítě v Roudnici n.L.



Testovací zapojení Fortigate 200F

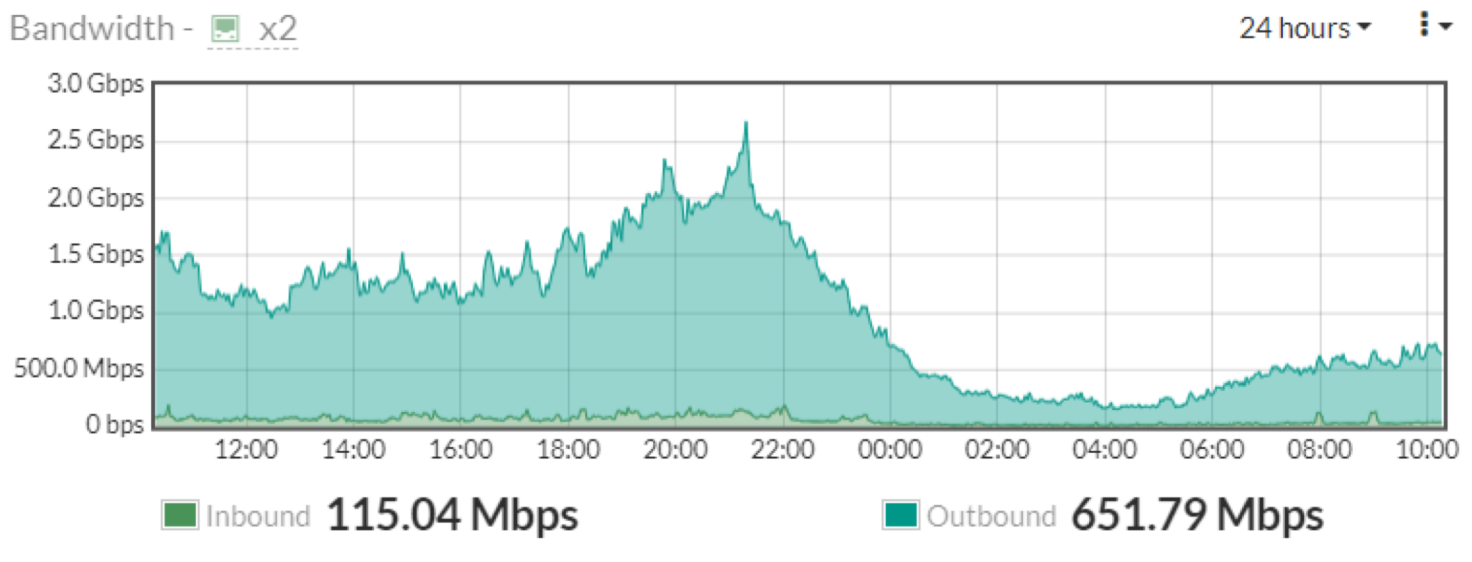
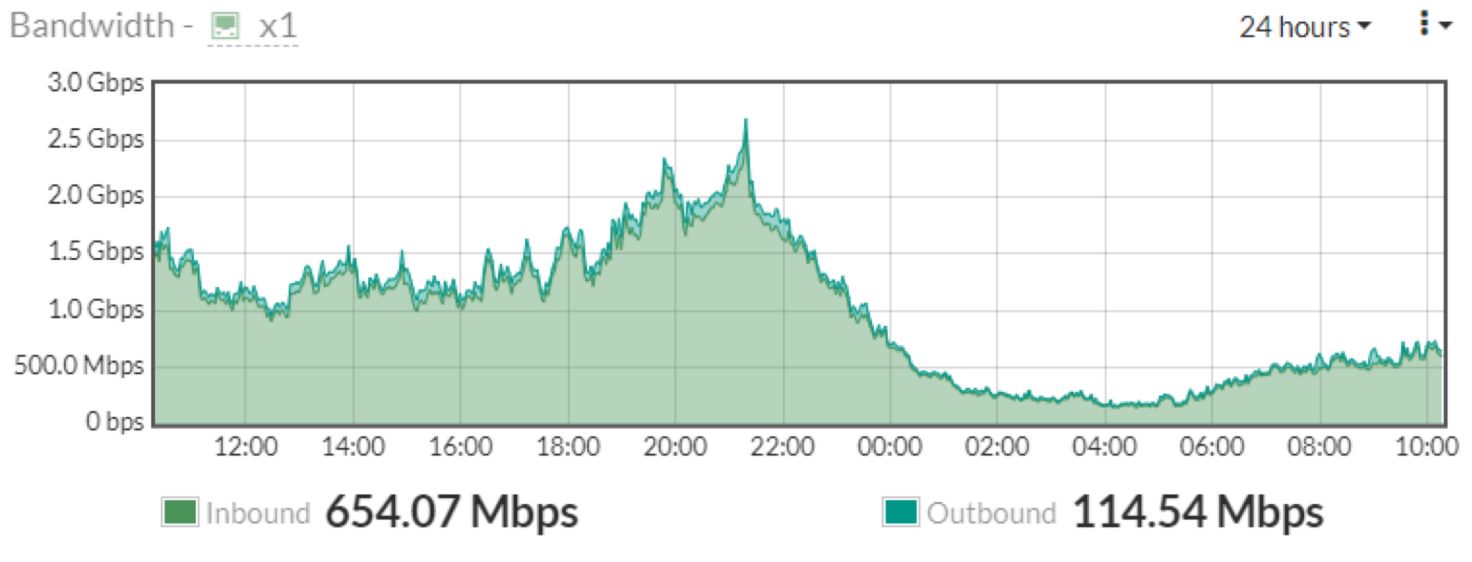


Finální zapojení Fortigate 200F



Konfigurace Fortigate 200F

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

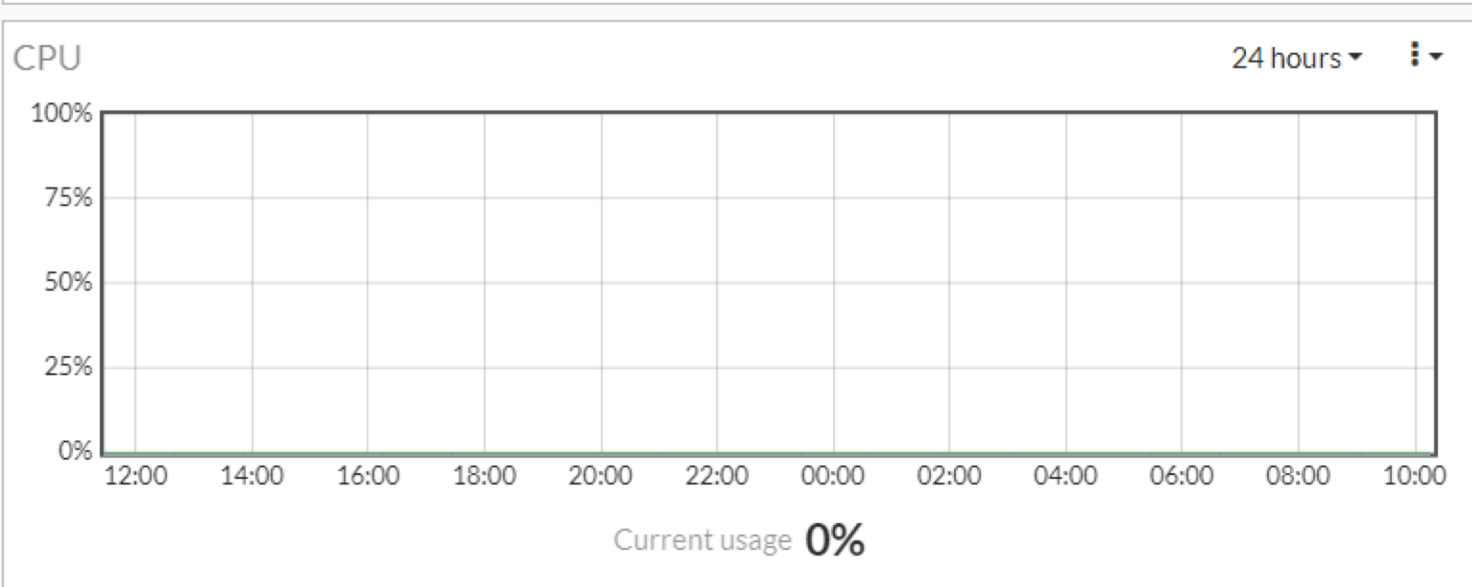
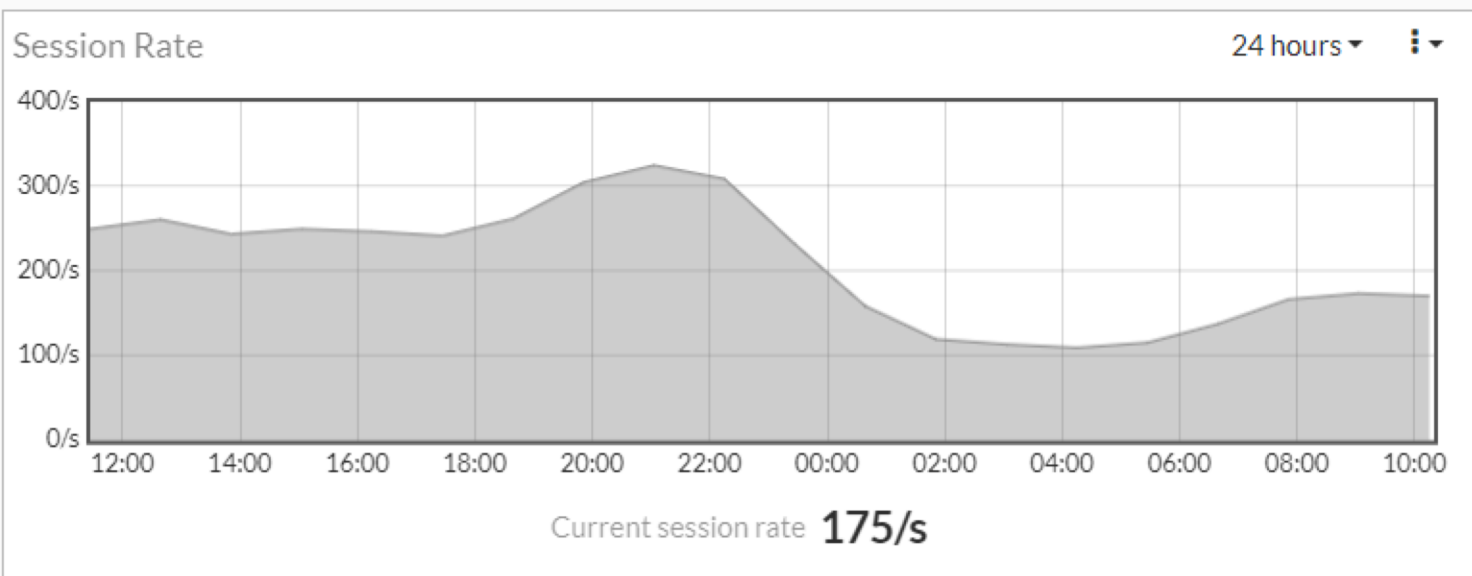


Graf provozu při testu

**Kumulativní provoz
Maximum Input
2,7Gbps**

**Maximum Output
2,7Gbps**





Graf vytížení CPU

**Maximum Session
310/s**

**Maximum CPU
0,5%**

✚ 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

Resources

Uptime: 249d 14:20:17

Free Memory: 3302.5 MiB

Total Memory: 3968.0 MiB

CPU: tilegx

CPU Count: 36

CPU Frequency: 1200 MHz

CPU Load: 7 %

Free HDD Space: 881.8 MiB

Total HDD Size: 1024.0 MiB

Architecture Name: tile

Board Name: CCR1036-8G-2S+

Version: 6.49.2 (stable)

Build Time: Dec/03/2021 14:53:53

Factory Software: 6.44

CPU

Find

CPU	Load (%)	IRQ (%)	Disk (%)
cpu12	16	16	0
cpu13	16	16	0
cpu14	16	16	0
cpu35	16	16	0
cpu8	15	15	0
cpu27	15	15	0
cpu29	14	14	0
cpu18	13	13	0
cpu28	12	11	0
cpu7	11	11	0
cpu15	11	11	0
cpu16	11	11	0
cpu20	11	11	0
cpu6	9	9	0
cpu10	8	8	0
cpu25	8	8	0
cpu31	8	8	0
cpu9	7	7	0
cpu23	7	7	0
cpu4	6	6	0
cpu32	6	6	0

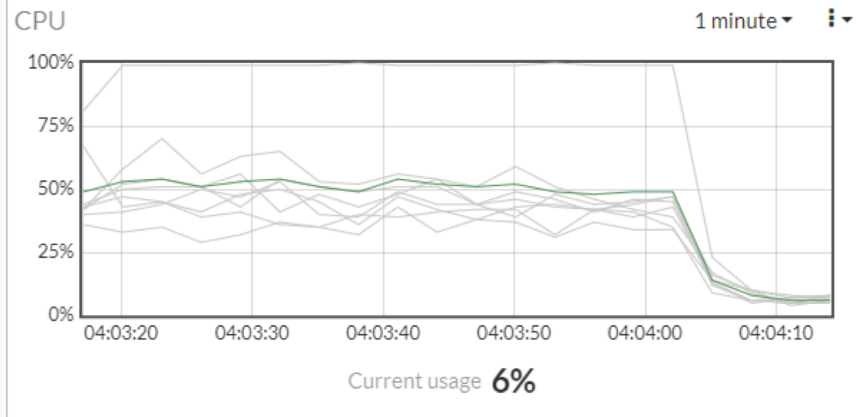
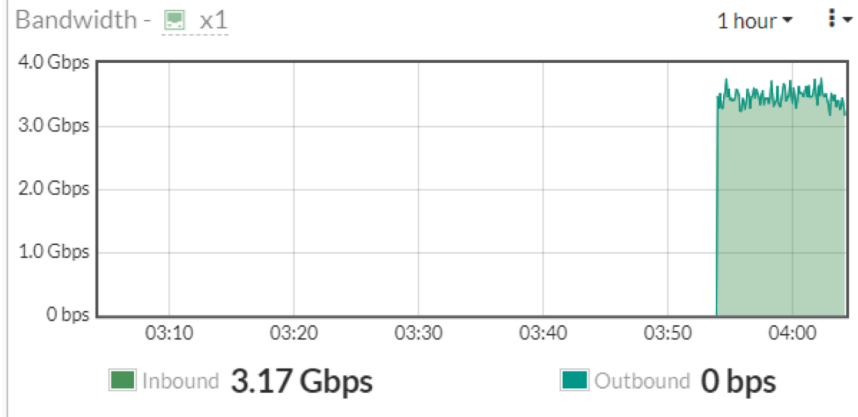
36 items

Graf vytížení CPU Mikrotik

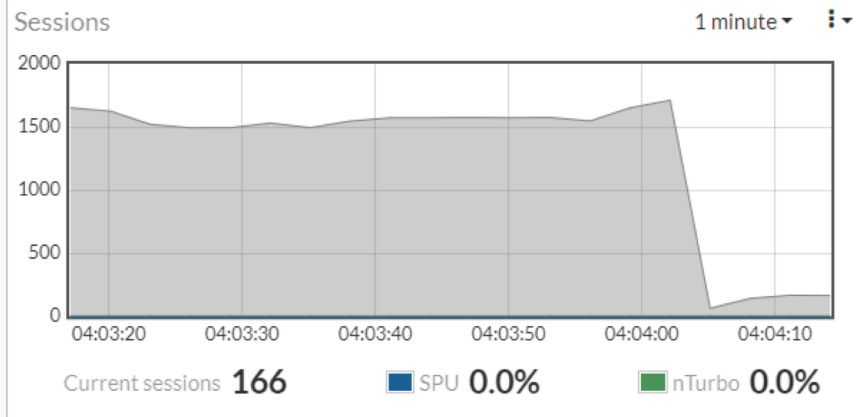
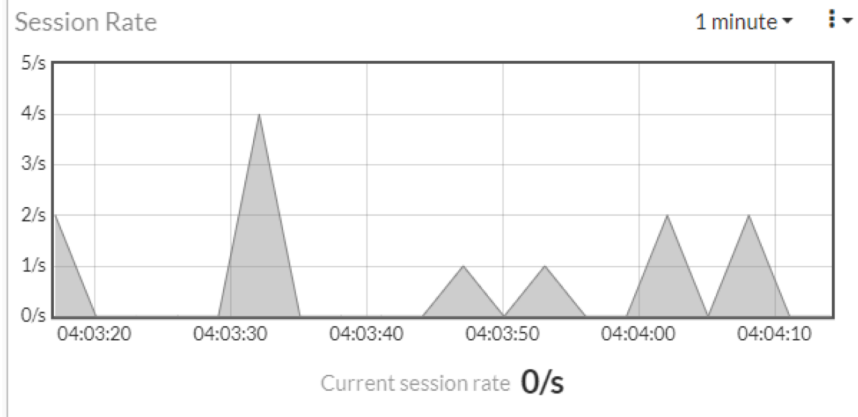
AVG 7%

MAX core CPU 16%

Vytížení CPU, nelegitimní provoz



**Maximum Input
3,2Gbps**



**AVG CPU
50%
Max core CPU
100%**

Fortigate jako zdroj NetFlow

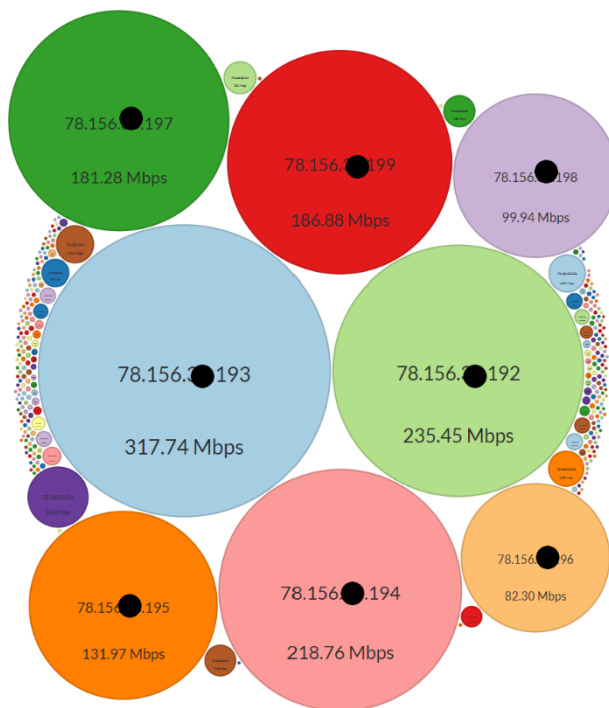
- Plný odběr hlaviček paketů
- Hardwarová podpora
- Konfigurace na více portů
- Plně vyhovuje potřebám DR

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**

Add Filter

Compare By: Bandwidth ▾



FG přehled provozu

**Aktuální provoz
[Mbps] na IP
adresách**

FortiView Sources by Bytes

now

Add Filter

Source	Device	Bytes	Sessions	Bandwidth
78.156.0.193		206.71 GB	7 107	232.37 Mbps
78.156.0.158		39.59 GB	1	1.12 Mbps
78.156.0.192		35.79 GB	6 873	283.76 Mbps
78.156.0.197		32.77 GB	4 215	255.42 Mbps
78.156.0.194		27.10 GB	4 455	191.46 Mbps

0% 300

FG přehled provozu

Aktuální provoz na IP adresách

78.156.xx.193

232 Mbps

7107 Sessions

206 GB



Destination	Application	Bytes ▾	Sessions ▾	Bandwidth ▾
ts0-seg.as.4net.tv (91.222.54.130)	TCP/443 TCP/80	8.90 GB	102	228.96 M...
ipv4-c001-vod001-cdtelematika-isp.1.oc...	TCP/443 TCP/80	17.02 GB	138	130.15 M...
cdn.fbsbx.com (157.240.30.27)	Facebook-Web (UDP/443)	4.06 GB	473	92.86 Mb...
scontent-prg1-1.cdninstagram.com (157...	Facebook-Web (UDP/443) Facebook-Instagram	3.24 GB	508	67.80 Mb...
vst05-3.o2tv.cz (83.208.217.25)	TCP/443	8.79 GB	17	27.00 Mb...
init-p01st.push.apple.com (2.21.74.97)	Apple-APNs (TCP/443)	973.92 MB	9	19.76 Mb...
nova-ott-vod-prep-prot.ssl.cdn.cra.cz (84...	TCP/80 TCP/443	2.56 GB	4	18.62 Mb...
vst23-3.o2tv.cz (83.208.217.79)	TCP/443	12.22 GB	14	18.61 Mb...
nova-ott-voyo-api.ssl.cdn.cra.cz (84.17.6...	TCP/80 TCP/443	2.66 GB	4	17.31 Mb...
ipv4-c002-vod001-cdtelematika-isp.1.oc...	TCP/80 TCP/443	1.84 GB	79	17.03 Mb...
d2nxq2uap88usk.cloudfront.net (65.9.95...	Amazon-AWS (TCP/443)	1.99 GB	14	16.52 Mb...
185.41.49.3	TCP/80	1.19 GB	7	15.93 Mb...

FG přehled provozu

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

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	Log Details
Minute ago	██████	31.30.164.55	17		clear_session	3 735	udp_flood	Source IP 31.30.164.55 Source Port 3294 Country/Region Czech Republic Source Interface x1 User
2 minutes ago	██████	185.24.21.5	17		clear_session	3 298	udp_flood	Destination IP 78.156.xx.196 Port 44073 Country/Region Czech Republic Destination Interface
3 minutes ago	██████	209.6.182.8	17		clear_session	3 130	udp_flood	Application Control Protocol 17 Service udp/44073
15 minutes ago	██████	178.255.168.41	17		clear_session	2 556	udp_flood	Action Action clear_session Threat 4096 Policy ID DDoS (1) Policy Type DoS IPv4
15 minutes ago	██████	178.255.168.41	17		clear_session	2 555	udp_flood	Security Level ████████ Threat Level Critical Threat Score 50
19 minutes ago	██████	118.193.58.78	17		clear_session	3 182	udp_flood	
28 minutes ago	██████	109.183.226.152	17		clear_session	2 674	udp_flood	
37 minutes ago	██████	31.23.154.215	17		clear_session	2 603	udp_flood	
43 minutes ago	██████	80.242.33.33	17		clear_session	3 574	udp_flood	
45 minutes ago	██████	81.200.55.229	17		clear_session	2 985	udp_flood	
51 minutes ago	██████	142.251.36.142	17		clear_session	4 976	udp_flood	
53 minutes ago	██████	87.197.113.77	17		clear_session	4 469	udp_flood	
55 minutes ago	██████	213.226.202.214	17		clear_session	2 602	udp_flood	
57 minutes ago	██████	46.114.161.157	17		clear_session	3 159	udp_flood	
Hour ago	██████	185.124.230.80	17		clear_session	2 667	udp_flood	
Hour ago	██████	93.99.5.58	17		clear_session	2 813	udp_flood	
Hour ago	██████	81.200.56.45	17		clear_session	2 722	udp_flood	
Hour ago	██████	212.79.110.114	17		clear_session	2 868	udp_flood	

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



Pokročilá analýza 2022-09-13 19:00 - 2022-09-13 22:50

STATISTIKA SEZNAM TOKŮ Předchozí výsledky 2022-09-14 11:01:18

Omezit na 20

Agregovat

Klepněte pro přidání položek

Zdrojová IPv4 maska 24

Cílová IPv4 maska 24

Radit podle toky

Použit zvolené kanály Použit všechny kanály v profilu

Výstup default + VYTVOŘIT NOVÝ VÝSTUP

FILTR

src ip 31.30.164.55

My filters <Žádný> ULOŽIT FILTR

ZPRACOVAT

All Sources
2022-09-13 19:00:00 - 2022-09-13 22:50:00
20 toky řadit podle Toky
src ip 31.30.164.55

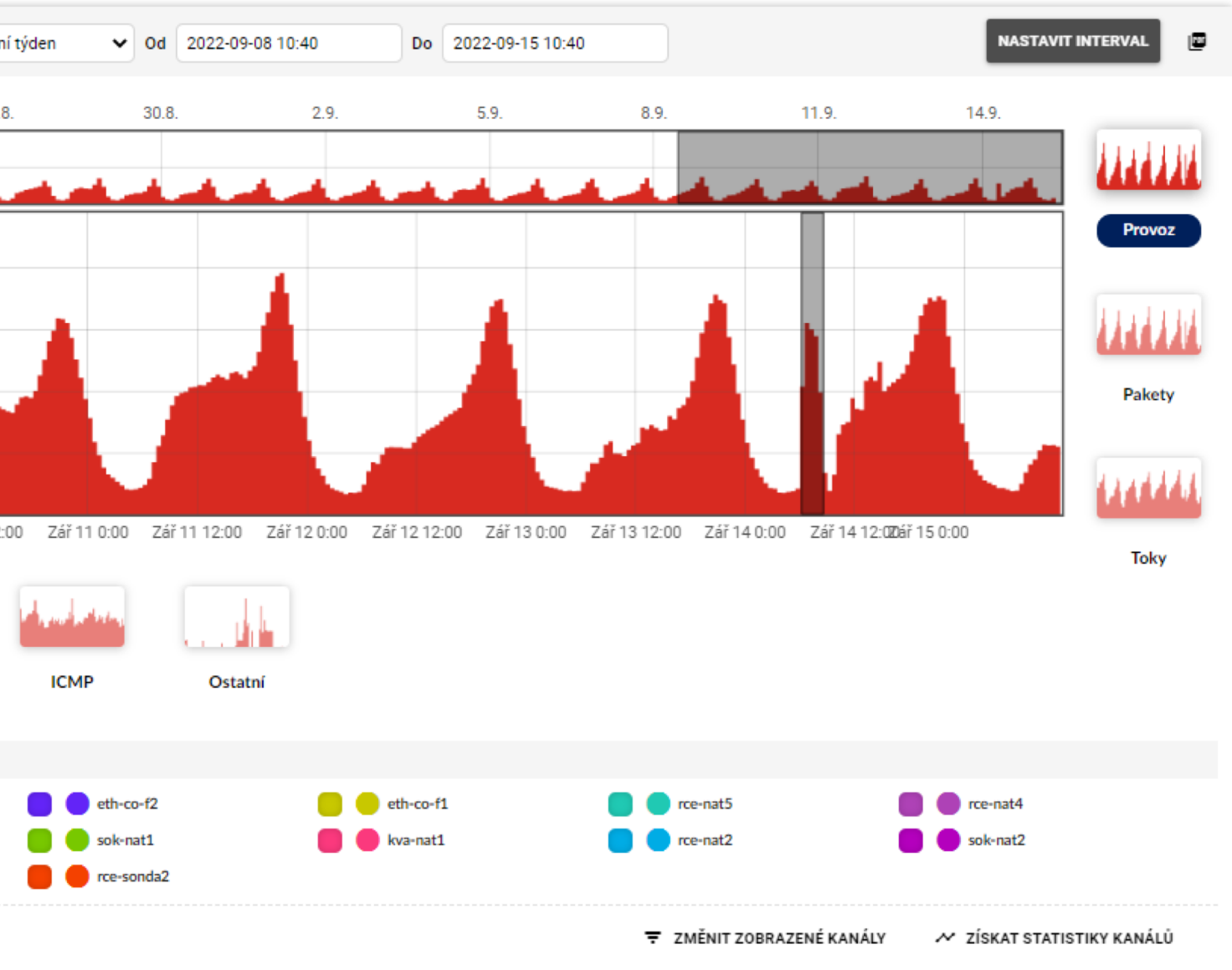
START TIME - FIRST SEEN	TRVÁNÍ	PROTOKOL	ZDROJOVÁ IP ADRESA	ZDROJOVÝ PORT	CÍLOVÁ IP ADRESA	CÍLOVÝ PORT	TCP PŘÍZNAKY	TOS	PAKETY	BAJTY	TOKY
2022-09-13 21:08:35.862	15.004 s	UDP	31.30.164.55	3294	78.156.30.196	44073	Best Effort & Default	157	19.01 KB	1
2022-09-13 21:08:35.110	14.91 s	UDP	31.30.164.55	3294	78.156.30.196	44073	Best Effort & Default	2.91 K	352.63 KB	1
2022-09-13 21:08:35.590	0.04 s	UDP	31.30.164.55	3294	78.156.30.196	9898	Best Effort & Default	0	0 B	1
Toky 3									Bajty 371.64 KB	Pakety 3.07 K	

Flowmon kolektor

Kontrola funkce DDoS ochrany na Flowmon kolektoru

Počet paketů: před FG 2910 za FG 157



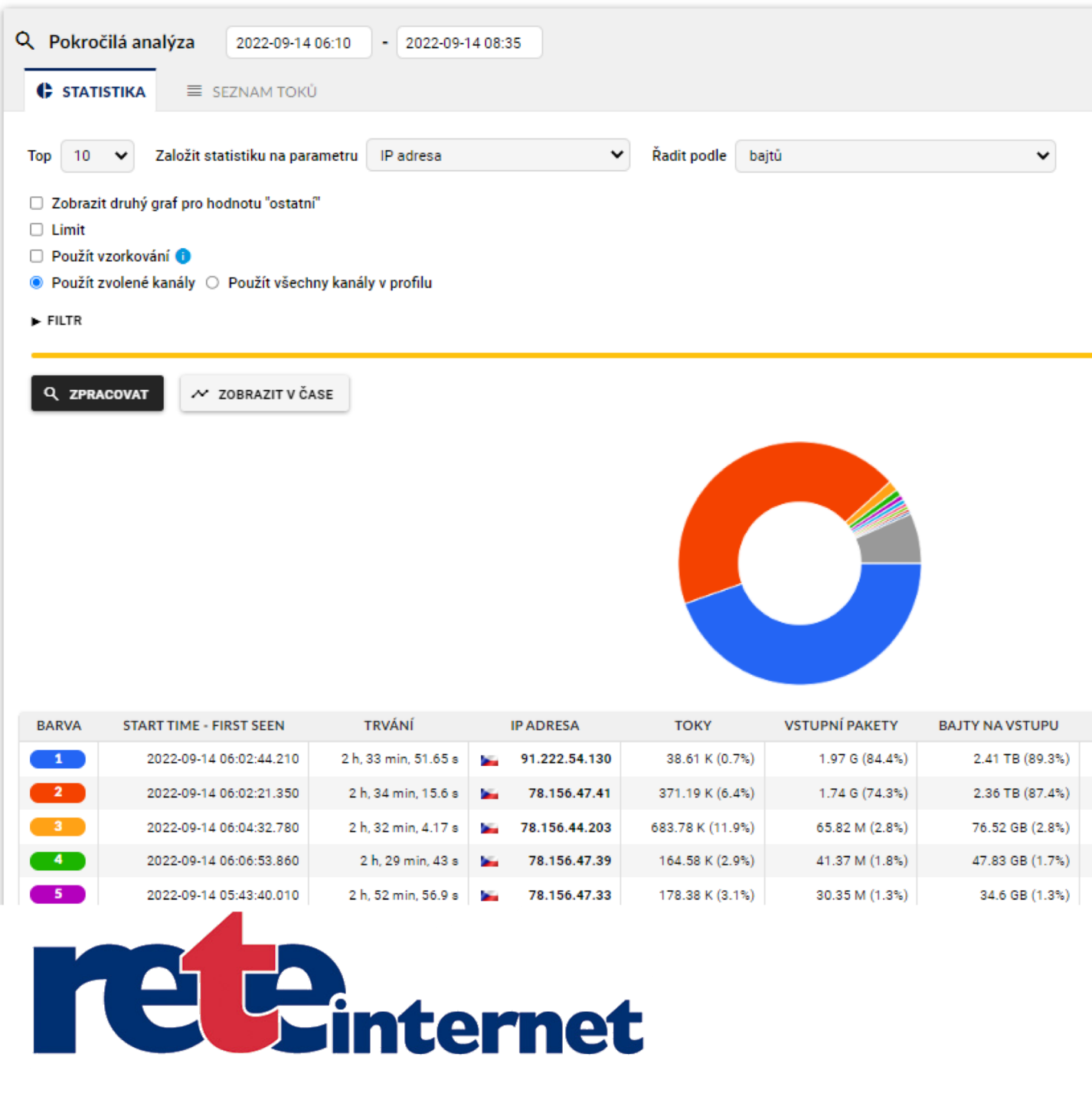


Flow kolektor

Běžná volumetrická kontrola provozu 7. dní zpět

Nalezení nestandardního provozu





Flow kolektor

Vyhledání příčiny nestandardního provozu pomocí statistiky

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

Pokročilá analýza 2022-09-14 06:10 - 2022-09-14 08:35

STATISTIKA SEZNAM TOKŮ Předchozí výsledky 2022-09-15 10:45:09

Omezit na 20

Agregovat

Zdrojová IP adresa Cílová IP adresa

Zdrojová IPv4 maska 24

Cílová IPv4 maska 24

Řadit podle bajtů

Použit zvolené kanály Použit všechny kanály v profilu

Výstup long + VYTVOŘIT NOVÝ VÝSTUP

FILTR

ip 91.222.54.130

My filters <Žádný>

ZPRACOVAT

Flow kolektor

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

All Sources
 2022-09-14 06:10:00 - 2022-09-14 08:35:00
 20 toků řadit podle Bajty
 ip 91.222.54.130

START TIME - FIRST SEEN	TRVÁNÍ	PROTOKOL	ZDROJOVÁ IP ADRESA	ZDROJOVÝ PORT	CÍLOVÁ IP ADRESA	CÍLOVÝ PORT	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	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	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	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	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	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	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	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	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	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	24
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	24
2022-09-14 06:40:34.180	44 min, 59.58 s	HOPOPT	ts0-seg.as.4net.tv	0	78.156.45.66	0	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	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	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	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	23

Nalezení spojení
 [4net a IPTV-NAT3]

Závěr
 Upgrade IPTV set-top-boxů



Flowmon kolektor & Fortigate komplexní monitoring

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

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

Komplexní projekt

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



Patrik Prešl

patrik.presl@rete.cz

reteinternet

 **GraphTech**