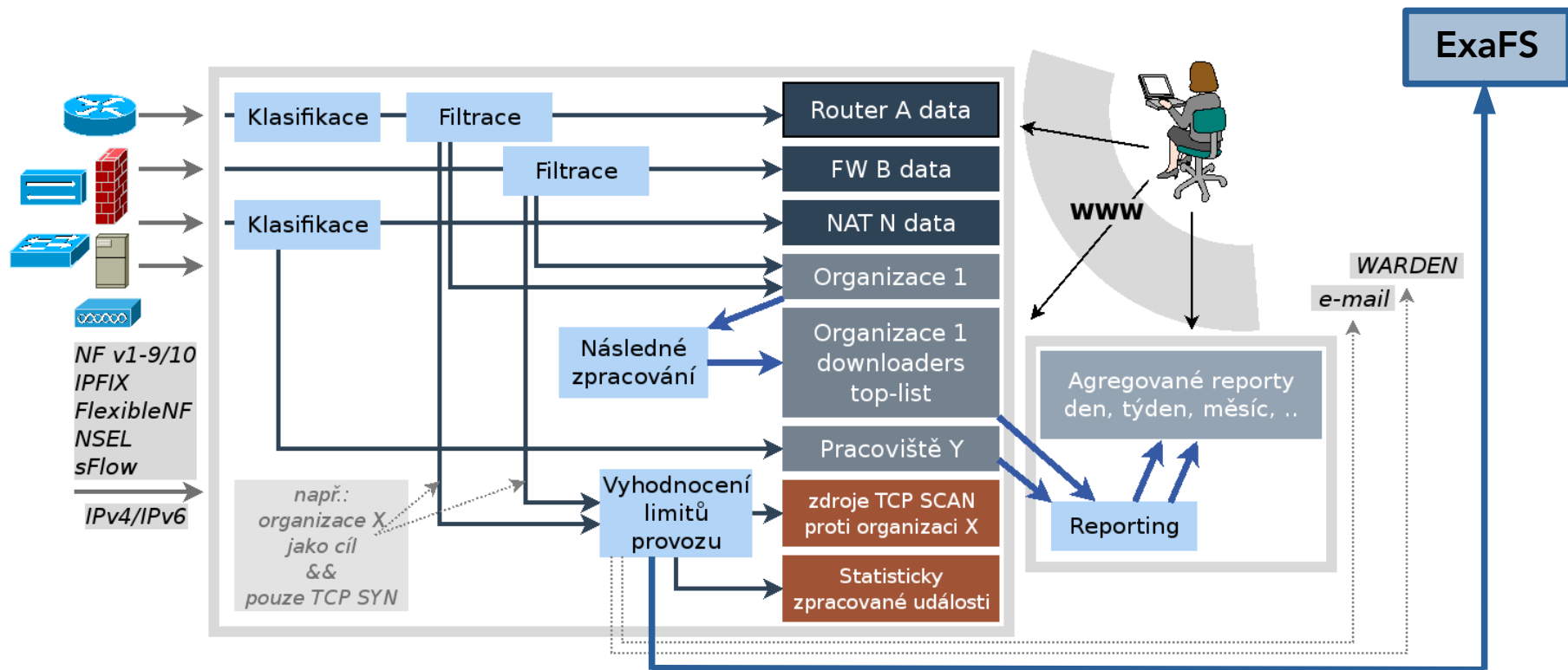


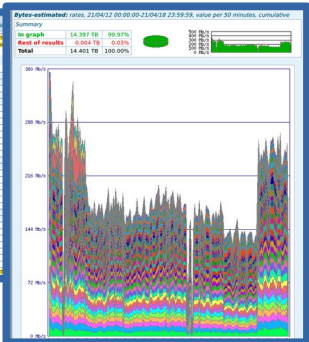
Use-cases z bezpečnostního monitoringu e-infrastruktury



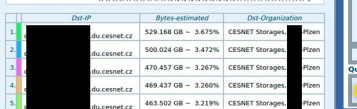
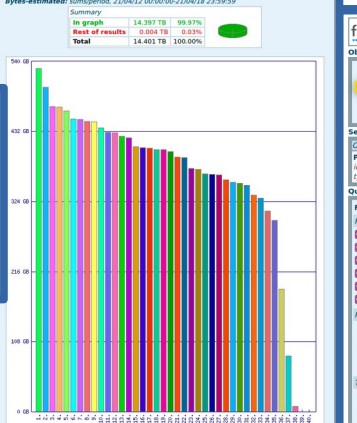
Tomáš Košnar, CESNET

- sběr, zpracování, uchování, zprostředkování informací o provozu v síti (na bázi toků)





```
tcp (6);https (443);50896;00000000;push(8)
tcp (6);https (443);50902;00000000;ack(16)
tcp (6);https (443);47316;00000000;push(8)
tcp (6);https (443);47320;00000000;fin(1), ack(16);1604;5;534.67
tcp (6);https (443);47364;00000000;ack(16);1500;1;1500
tcp (6);https (443);47352;00000000;ack(16);1500;1;1500
001:718;x:100:x:x:x;tcp (6);https (443);40546;00000000;syn(2), push
001:718;x:100:x:x:x;udp (17);domain (53);55375;00000000;;171;1;171
```



Tas esnet version 21.05 (v1.9, Flex/NF, NSEL, NSFlow, SFlow, Tom Kozar, CESNET A.S.)

Primary installation in CESNET e-infrastructure

Query **Viewer** **System Statistics** **Configuration** **Reports** **FATS NSOC** **Help and info**

Select Selection ...?

Filter	Any object type	... filtering	in name.
Praha1	☒	router	(NIX)
Praha1	☒	router	(AKA/NF, CEANT, L..)
Praha1	☒	router	(NIX)
Praha1	☒	router	(NIX) Public

Personal Object-Sets Management
Save objects as ObjectSet
Load or update ... select objects set = ... → delete
Objects information ... standard

Selected Objects Information

Object:
Praha1 ... backbone, border router (NIX) **Public internet**

Active Data
PRIMARY: table size=10 minutes, history=183 days, aggregation=None
Oldest data table: 2020/10/21 09:00:00 ... real history ~ 183 days

Type=Flow Data Source

Query Parameters ...?

Fields to store in results ...? you can switch to "Generic" condition form

Flow Src/Dst Fields

Do up	Do down
☒ Src-Port	☒ Dst-Port
☒ Src-Index	☒ Dst-Index
☒ Ingress-VRFID	☒ Egress-VRFID
☒ Src-Prev-AS	☒ Dst-Next-AS
☒ Src-Bitmask	☒ Dst-Bitmask

Flow Common Fields

Flow Direction	Flow Status	Flow Data Source
☒ Protocol	☒ TCP-Flags	☒ Hopup
☒ TOS-Flags	☒ Flow-Duration	☒ Bytes-measured

Time, Value and Count Fields

Flow Start	Pkts-measured
☒ Flow-End	☒ Pkts-estimated
☒ Bytes-measured	☒ Flow-Cnt
☒ Bytes-estimated	

Fields Query Condition - Simple Form ...?

Query traffic (in form below) ☒ from Source to Destination ☐ bidirectional ☐ from Destination to Source

Source	Relation	Destination
IP address	and	
Service Port	and	
AS Number	and	
Interface Index	and	
VRFID	and	

TCP-flags	TOS-flags	Flow-Direction
ack	critic_eop	egress
fin	flash	ingress
push	high_reliability	

Protocol: 255, 25, dcp

Flow Direction: FWD>Status

Query Condition Management

Save condition as Condition
Load or update ... select condition ... time params. ... delete

Time Parameters ...?

-10 minutes -> -now GMT time cut flows at time interval border
...optional sub-aggregation period (corresponding with graphs in seconds) = -into ...?
...optional data table sampling (must be integer value): will be auto-connected to query at least 3 data tables = -to ...?

Aggregation ...? "group by" clause applied on each source data table (depends on "selected fields" and "table size" values)...?

Query Processing ...?

Run New Query ...
Max. duration [30 seconds]
Max. count [20000 records]
Background processing []
Notify to (e-mail) []
Query name (when "Run New Query"): []

- **potřeba nalézt charakteristiku útoku** – k dispozici čas, cílový prefix, dopad (přetížení/zahlcení hraničního prvku)
- **příklad postupu**
 - 1) vyhledání provozních informací pro daný cílový prefix, těsně okolo času výpadku
 - 2) vizualizace → různé top-listy s různou mírou detailu (od obecného k detailnímu), třídění + doplňující informace → hledání významného „informačního prvku“
→ nalezena 1 cílová adresa, odhad na tcp syn-flood

0 >	Dst-IP	Protocol	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt
1.		2 tcp (6)	253.475 MB ~ 24.626% → 959.940 Kb/s	3.550 Mp ~ 64.493% → 1.680 Kp/s	64.40	843477 ~ 97.520% → 399.294 flows/s
2.		2 icmp (1)	51.714 MB ~ 5.024% → 195.219 Kb/s	765.091 Kp ~ 13.900% → 361.022 p/s	67.41	2964 ~ 0.343% → 1.399 flows/s
3.		8 tcp (6)	113.299 MB ~ 11.007% → 429.501 Kb/s	314.000 Kp ~ 5.705% → 148.791 p/s	357.22	2504 ~ 0.290% → 1.187 flows/s
4.		6 udp (17)	156.963 MB ~ 15.250% → 602.253 Kb/s	260.453 Kp ~ 4.732% → 124.917 p/s	613.77	2001 ~ 0.231% → 0.960 flows/s
5.		8 udp (17)	183.617 MB ~ 17.839% → 749.309 Kb/s	234.590 Kp ~ 4.262% → 119.665 p/s	781.53	2482 ~ 0.287% → 1.266 flows/s
6.		5 udp (17)	61.207 MB ~ 5.946% → 236.290 Kb/s	146.878 Kp ~ 2.668% → 70.879 p/s	416.85	1378 ~ 0.159% → 0.665 flows/s
7.		5 tcp (6)	105.861 MB ~ 10.285% → 407.635 Kb/s	97.422 Kp ~ 1.770% → 46.892 p/s	1092.43	1473 ~ 0.170% → 0.709 flows/s
8.		9 tcp (6)	70.748 MB ~ 6.873% → 291.868 Kb/s	76.062 Kp ~ 1.382% → 39.224 p/s	931.73	525 ~ 0.061% → 0.271 flows/s
9.		6 tcp (6)	26.821 MB ~ 2.606% → 102.058 Kb/s	36.006 Kp ~ 0.654% → 17.126 p/s	718.58	1713 ~ 0.198% → 0.815 flows/s
10.		6 udp (17)	589.545 KB ~ 0.057% → 2.247 Kb/s	6.441 Kp ~ 0.117% → 3.069 p/s	87.17	2990 ~ 0.346% → 1.425 flows/s
Left			5.001 MB ~ 0.486%	17.521 Kp ~ 0.318%		
0 >	Dst-IP	Protocol	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt

1. ověření syn-flood - např. agregace: **proto=6(tcp)** and **tcp_flags=2(SYN)** and **tcp_flags<>16(ACK)**

o	Dst-IP	Protocol	TCP-flags	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Dst-IP-Cnt	Src-Port-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
1.		tcp (6)	syn(2), rst(4)	125.691 MB	1.766 Mp	353467	1	65419	65425	64.00	421651

2. porovnání vůči celkovému objemu tcp - agregace: **proto=6(tcp)**

o	Dst-IP	Protocol	TCP-flags	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Dst-IP-Cnt	Src-Port-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
1.		tcp (6)	fin(1), syn(2), rst(4), push(8), ack(16)	253.475 MB	3.550 Mp	619858	1	65535	65535	64.40	843477

▪ vysvětleno cca 50%, zkusme tedy test výskytu toků s nastavenými SYN a zároveň ACK

3. agregace: **proto=6(tcp)** and **tcp_flags=2(SYN)** and **tcp_flags=16(ACK)**

o	Flow-Direction	FWD-Status	Dst-IP	Protocol	TOS-flags	TCP-flags	Bytes-estimated	Avr-Pkt-Length	Flow-Cnt
1.	egress	Forwarded not Fragmented		tcp (6)	00100100	syn(2), ack(16)	125.646 MB	64.00	421251

4. zkusme ověřit opačný směr přenosu: **proto=6** and **tcp_flags=16**

o	Protocol	TCP-flags	Bytes-estimated	Pkts-measured	Pkts-estimated	Src-IP-Cnt	Dst-IP-Cnt	Src-Port-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
1.	tcp (6)	fin(1), syn(2), rst(4), push(8), ack(16)	18.500 MB	9.897 Kp	20.809 Kp	1	83	11	385	882.62	522

5. ..a **proto=6** and **tcp_flags<>16**

o	Protocol	TCP-flags	Bytes-estimated	Pkts-estimated	Dst-IP-Cnt	Src-Port-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
1.	tcp (6)	syn(2), rst(4)	23.931 MB	529.410 Kp	141309	58965	59104	40.00	151582

▪ z proporce a počtu zpětných toků můžeme usuzovat umělé generování SYN + ACK ze strany útočníka

- a ICMP z úvodního top-listu ?

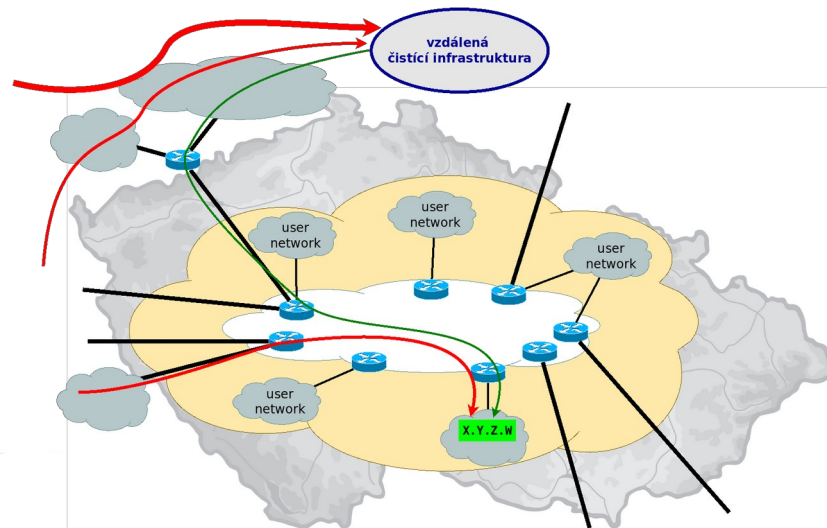
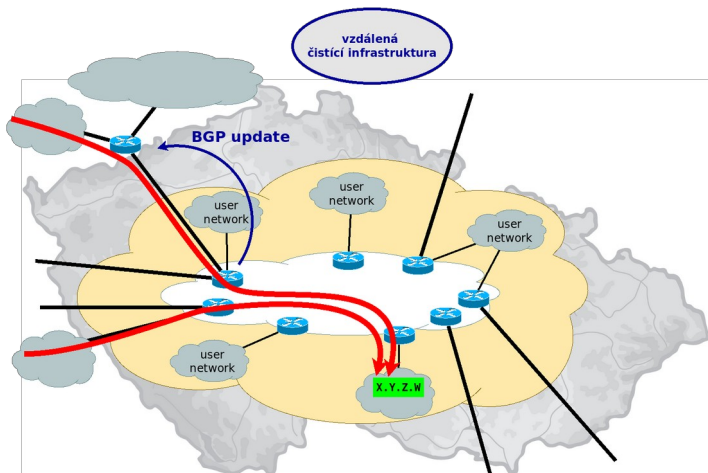
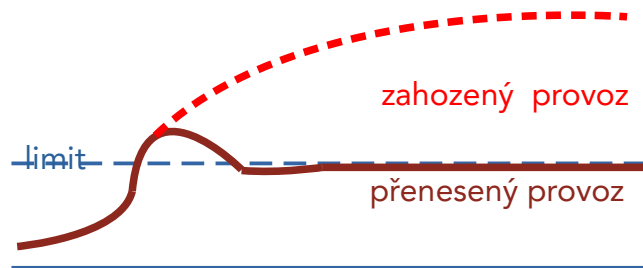
o	>	Dst-IP	Protocol	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt
1.			2 tcp (6)	253.475 MB ~ 24.626% → 959.940 Kb/s	3.550 Mp ~ 64.493% → 1.680 Kp/s	64.40	843477 ~ 97.520% → 399.294 flows/s
2.			2 icmp (1)	51.714 MB ~ 5.024% → 195.219 Kb/s	765.091 Kp ~ 13.900% → 361.022 p/s	67.41	2964 ~ 0.343% → 1.399 flows/s



o	Dst-IP	Protocol	Dst-Port	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Avr-Pkt-Length	Flow-Cnt
1.		2 icmp (1)	Host Unreachable (769)	26.076 MB	383.112 Kp	931	67.93	1557
2.		2 icmp (1)	Time to Live exceeded in Transit (2816)	23.528 MB	350.943 Kp	444	66.80	1053
3.		2 icmp (1)	Net Unreachable (768)	1.895 MB	27.873 Kp	52	67.87	88
4.		2 icmp (1)	Communication Administratively Prohibited (781)	86.518 KB	1.333 Kp	50	63.76	58
5.		2 icmp (1)	Port Unreachable (771)	62.001 KB	900.000 p	48	66.68	51
6.		2 icmp (1)	Communication with Destination Host is Administratively Prohibited (778)	58.390 KB	797.000 p	133	68	138
7.		2 icmp (1)	Echo-request (2048)	5.765 KB	71.000 p	10	79.59	10
8.		2 icmp (1)	Redirect Datagram for the Network (or subnet) (1280)	1.800 KB	31.000 p	2	56	3
9.		2 icmp (1)	Redirect Datagram for the Host (1281)	2.267 KB	31.000 p	6	66.67	6

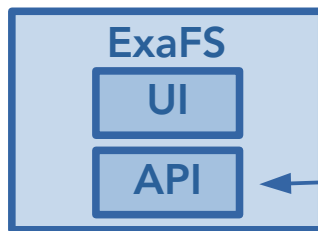
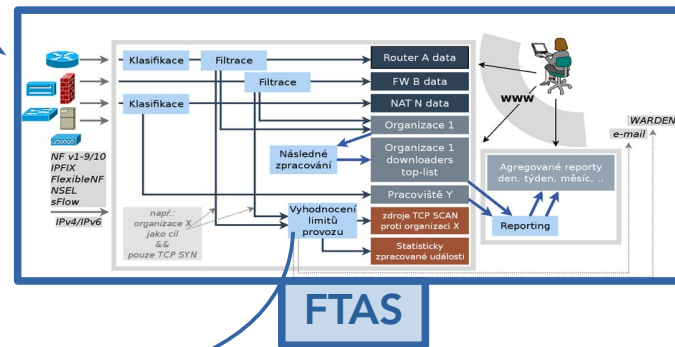
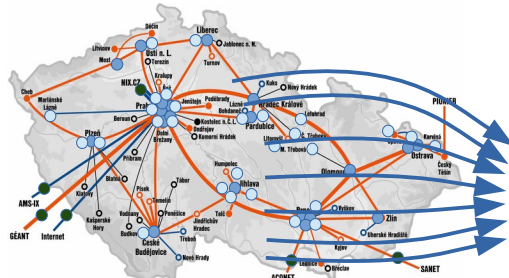
- shrnutí
 - celkový čas v tomto případě – vyhledání provozu + (vizualizační, vysvětlující) analytika ~ 10 minut
 - obdobné požadavky nebo nutnost analýzy na základě bezpečnostních hlášení jsou standardem
 - přesnost zadání → efektivita
 - vývoj nástrojů musí jít tomuto typu činnosti „naproti“
 - lidé + znalosti !!!

- příklad útoku na bázi amplifikace/odrazu
- uplatněné prvky obrany
 - policing na perimetru
 - vzdálené čištění



Use-case 2: automatická regulace provozu

- příklad útoku na bázi amplifikace/odrazu
- FTAS: monitoring, detekce
- ExaFS: řízení provozu



síťová část e-infrastruktury

- notifikace systému FTAS

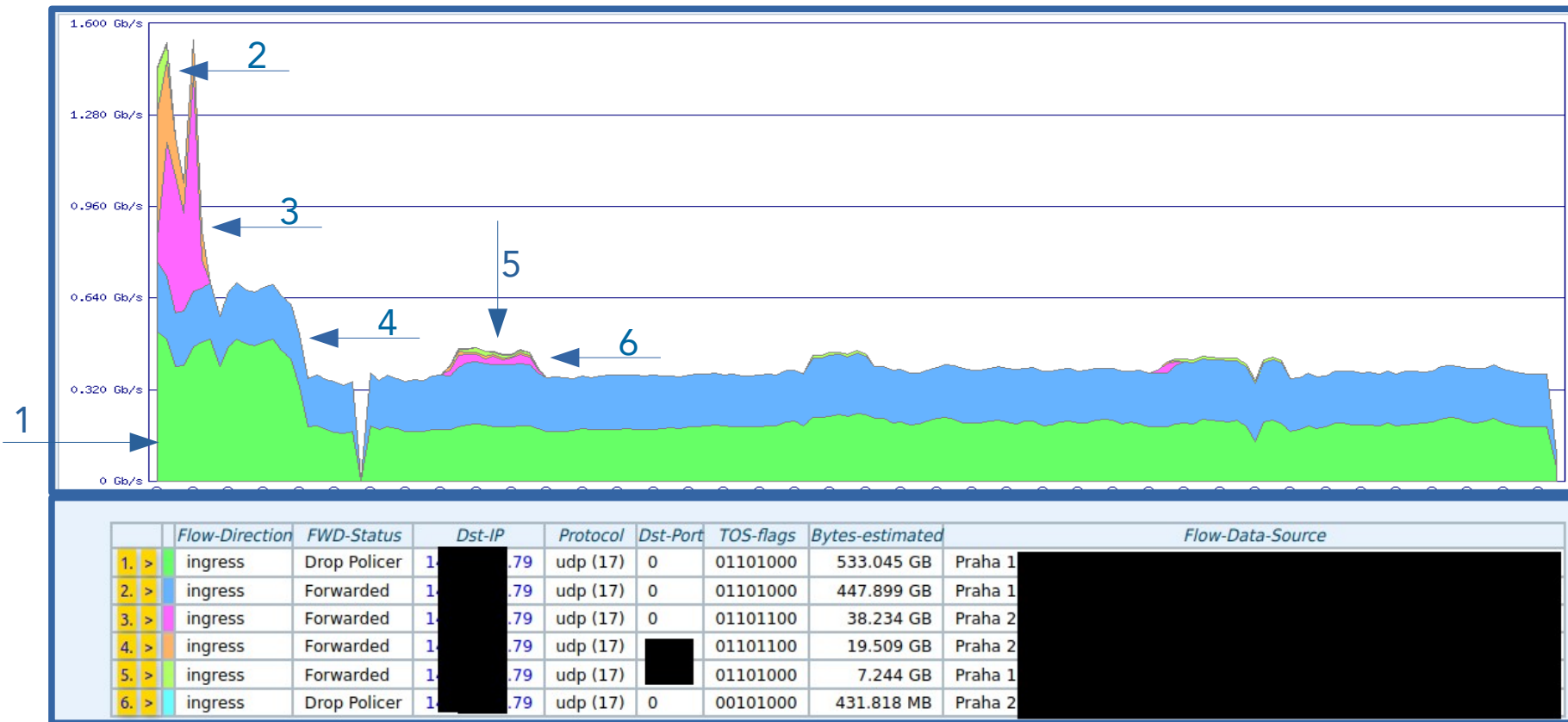
```
Notification : 1 [REDACTED] (Dst-IP) - 'IPv4 UDP amplification, reflection - targets internal' - 1. DETECTED, 98.46% traffic drops
Handling      : none
Events        : 3 events detected

Summary, overview
Duration      : 43.962 seconds within [REDACTED]
Data sources  : Praha 1 [REDACTED]
Flows         : 46.000 flows, 1.046 flows/s, 60.87% drops
Pkts          : 12.432 Mp, 0.283 Mp/s, 93.35% drops
Bytes         : 16.951 GB, 3.085 Gb/s, 1363.519 Bpp, 93.29% drops

Current event
Duration      : 28.962 seconds within [REDACTED]
Data source   : Praha 1 [REDACTED]
Flows         : 13.000 flows, 0.449 flows/s, 61.54% drops
Pkts          : 4.448 Mp, 0.154 Mp/s, 98.46% drops
Bytes         : 6.065 GB, 1.675 Gb/s, 1363.665 Bpp, 98.43% drops
Src-IP/6      : [REDACTED] 0.202, [REDACTED] 72.252, [REDACTED] 211.222, [REDACTED] 29.4, [REDACTED] 5.65, [REDACTED] 233.166
Dst-IP/1       : 1 [REDACTED]
Protocol/1    : udp
Src-Port/1    : 0
Dst-Port/1    : 0
Src-ifIndex/2 : 173 (Bundle-Ether [REDACTED]) (Bundle-Ether1
Dst-ifIndex/2 : 0, 175 (HundredGig [REDACTED])
```

- součástí hlášení informace o úspěšném automatickém přesměrování na vzdálené čištění

- průběh útoku, ex-post analýza/vizualizace



- příklad útoku na bázi amplifikace/odrazu 2
- notifikace systému FTAS

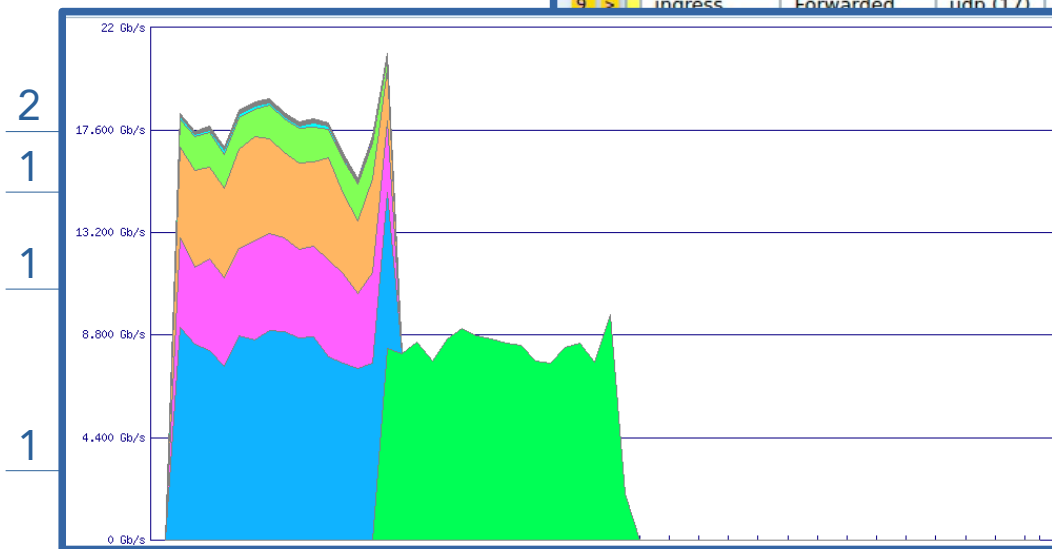
```
Notification      : [REDACTED] (Dst-IP) - 'IPv4 UDP amplification, reflection - targets internal' - 1. DETECTED, 99.58% traffic drops
Handling         : none
Events          : 1 event detected

Current event
Duration        : 30.000 seconds within [REDACTED]
Data source     : Praha [REDACTED] (Public Internet)
Flows           : 22.347 Kflows, 0.745 Kflows/s, 87.30% drops
Pkts           : 81.765 Mp, 2.726 Mp/s, 99.58% drops
Bytes          : 38.116 GB, 10.164 Gb/s, 466.168 Bpp, 99.58% drops
Src-IP/64+     : [REDACTED]
1.52.216.241, 1.53.[REDACTED]
Dst-IP/1       : [REDACTED]
Protocol/1     : udp
Src-Port/1     : [REDACTED]
Dst-Port/6     : [REDACTED]
```

- součástí hlášení informace o úspěšném automatickém přesměrování na vzdálené čištění

- průběh útoku, ex-post analýza, vizualizace

	Flow-Direction	FWD-Status	Protocol	Src-Port	Src-ifIndex	TOS-flags	Bytes-estimated	Pkts-estimated
1. >	ingress	Forwarded	udp (17)				111	169.608 GB
2. >	ingress	Drop Policer	udp (17)				111	153.709 GB
3. >	ingress	Drop Policer	udp (17)				100	71.269 GB
4. >	ingress	Drop Policer	udp (17)				100	71.007 GB
5. >	ingress	Drop Policer	udp (17)				000	25.255 GB
6. >	ingress	Drop Policer	udp (17)				000	2.085 GB
7. >	ingress	Forwarded	udp (17)				000	896.979 MB
8. >	ingress	Forwarded	udp (17)				100	784.631 MB
9. >	ingress	Forwarded	udp (17)				111	641.307 MB
							100	371.634 MB
							000	325.359 MB
							000	182.745 MB
							000	77.500 KB
								164.000 p



..nesmíme podléhat pokušení, že jedno řešení nás spasí.. ;-)

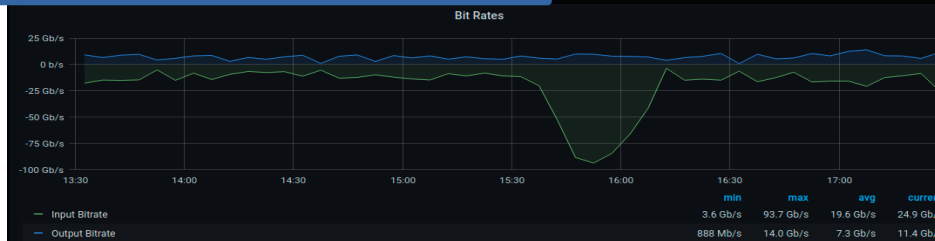
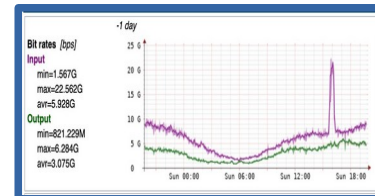
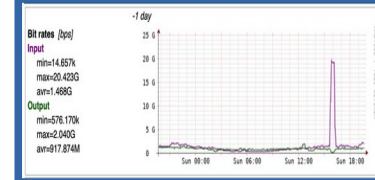
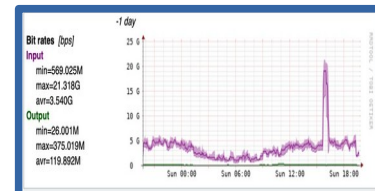
Use-case 4: charakteristika významného útoku

- amplifikační útok - počet reflektorů, amplifikační koeficient, struktura

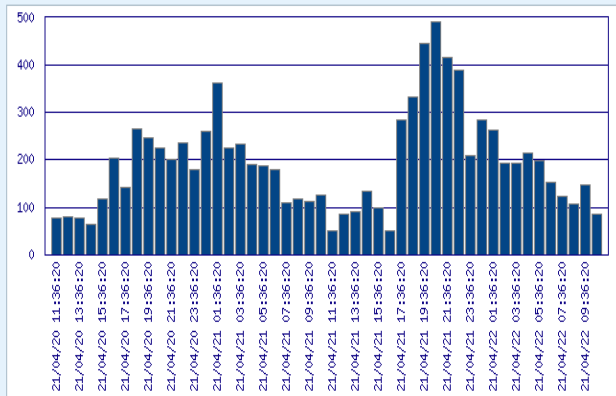
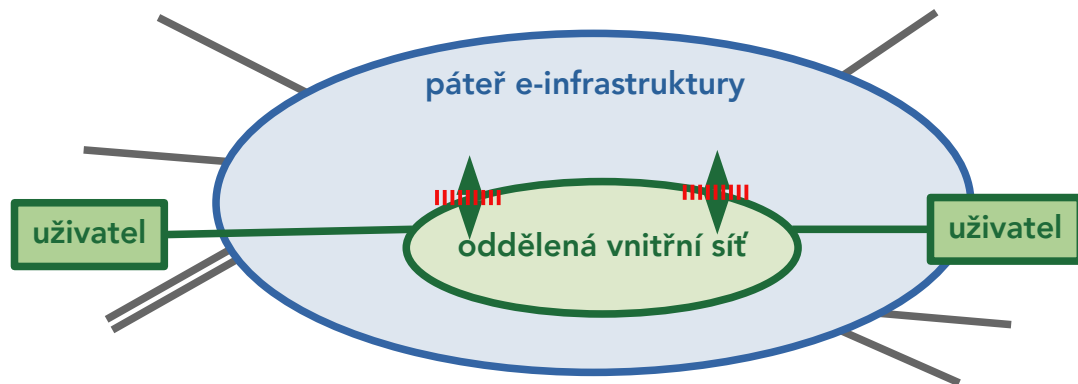
o	Flow-Direction	Protocol	Bytes-estimated	Pkts-estimated	Src-IP-Cnt
1.	ingress	udp (17)	1.537 TB	1.229 Gp	77560

o	FWD-Status	Protocol	Src-Port	TOS-flags	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length
1.	Drop Policer	udp (17)	0	11111111	1.580 TB ~ 55.931%	1.277 Gp ~ 58.998%	1240.19
2.	Drop Policer	udp (17)	domain (53)	11111111	1.121 TB ~ 39.677%	791.005 Mp ~ 36.545%	1420.33
3.	Forwarded	udp (17)	0	11111111	66.598 GB ~ 2.358%	53.634 Mp ~ 2.478%	1241.90
4.	Forwarded	udp (17)	domain (53)	11111111	57.187 GB ~ 2.024%	42.341 Mp ~ 1.956%	1363.34
5.	Forwarded	udp (17)	145	00000000	43.818 MB ~ 0.002%	29.212 Kp ~ 0.001%	1500
6.	Forwarded	udp (17)	166	00000000	27.624 MB ~ 0.001%	18.416 Kp ~ 0.001%	1500
7.	Forwarded	udp (17)	46069	00000000	26.194 MB ~ 0.001%	17.556 Kp ~ 0.001%	1492
8.	Forwarded	udp (17)	61016	00000000	23.622 MB ~ 0.001%	15.748 Kp ~ 0.001%	1500
9.	Forwarded	udp (17)	312	00000000	22.170 MB ~ 0.001%	14.780 Kp ~ 0.001%	1500
10.	Forwarded	udp (17)	46066	00000000	20.912 MB ~ 0.001%	14.016 Kp ~ 0.001%	1492
11.	Forwarded	udp (17)	codaaauth2 (370)	00000000	17.400 MB ~ 0.001%	11.600 Kp ~ 0.001%	1500
12.	Forwarded	udp (17)	165	00000000	15.750 MB ~ 0.001%	10.500 Kp ~ 0.000%	1500
13.	Forwarded	udp (17)	echo (7)	00101000	13.320 MB ~ 0.000%	8.880 Kp ~ 0.000%	1500

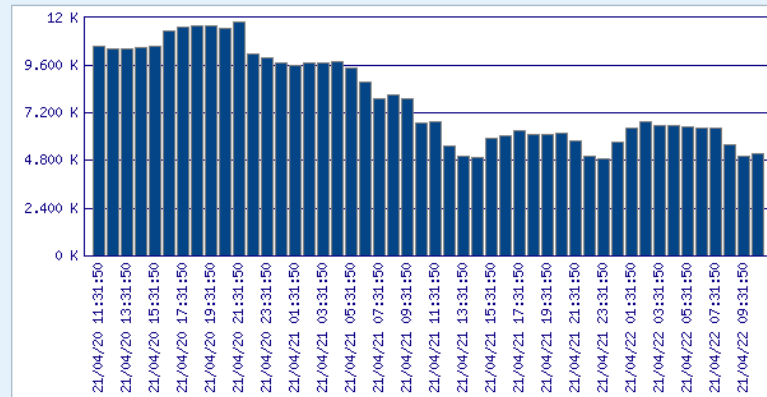
- s provozem zahojeným v předchozích sítích celkově cca 120+ Gb/s



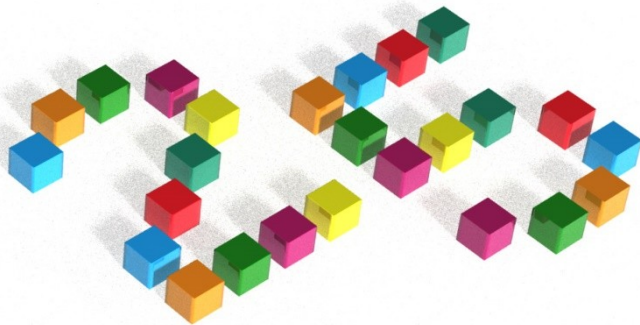
- hSOC
- dvoustupňové řešení
- komplementární nastavení
- sumarizace



Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
85.538 GB	85.538 GB	1.281 Gp	1.281 Gp	770	3934312	108293	9267	Src-IP



Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
3.146 GB	78.283 Mp	778	78343742	77591423	381270	Src-IP



..poděkování celé komunitě za spolupráci a zpětnou vazbu při tvorbě a optimalizaci nástrojů a technik obrany..

Děkuji za pozornost!



Use-cases z bezpečnostního monitoringu e-infrastruktury