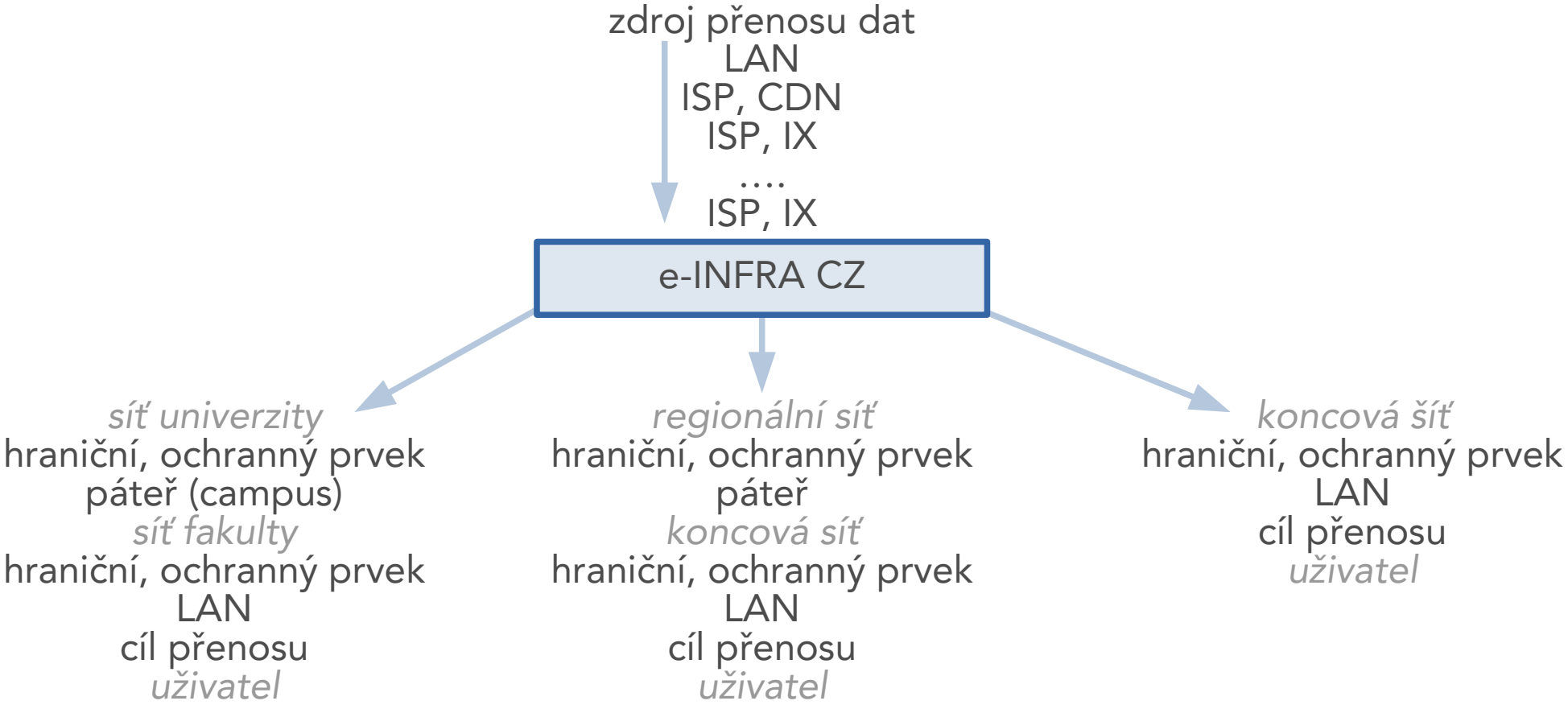
cesnet

Aktuality z monitoringu a zabezpečení sítě e-INFRA CZ

Tomáš Košňar
CESNET

Seminář o bezpečnosti sítí a služeb
9. 2. 2021

o čem to bude...

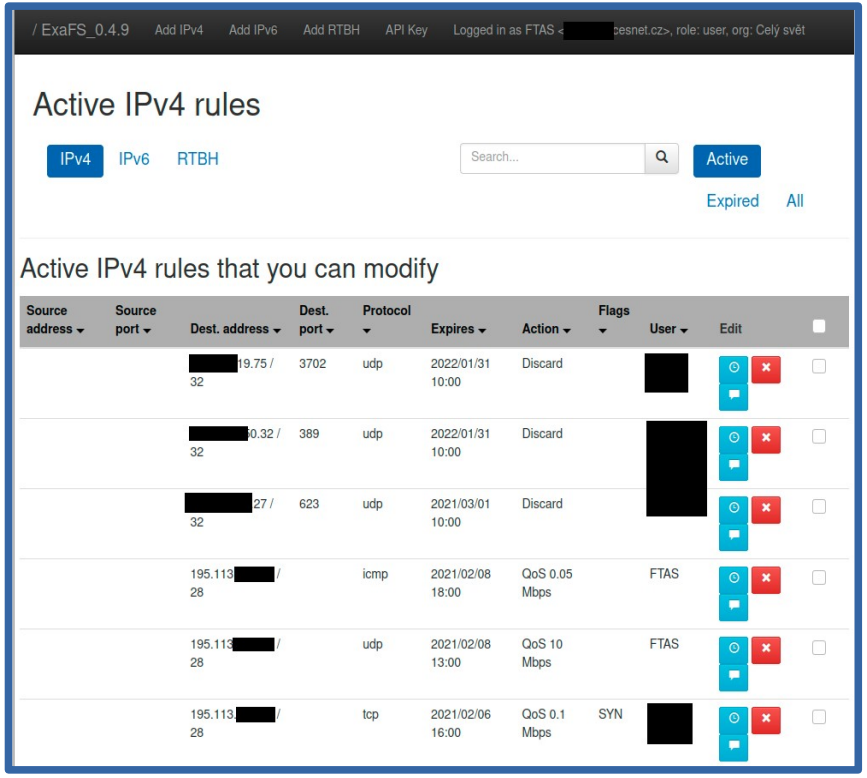

zdroj přenosu dat
LAN
ISP, CDN
ISP, IX
....
ISP, IX
e-INFRA CZ
síť univerzity
hraniční, ochranný prvek
páteř (campus)
síť fakulty
hraniční, ochranný prvek
LAN
cíl přenosu
uživatel
regionální síť
hraniční, ochranný prvek
páteř
koncová síť
hraniční, ochranný prvek
LAN
cíl přenosu
uživatel
koncová šíť
hraniční, ochranný prvek
LAN
cíl přenosu
uživatel

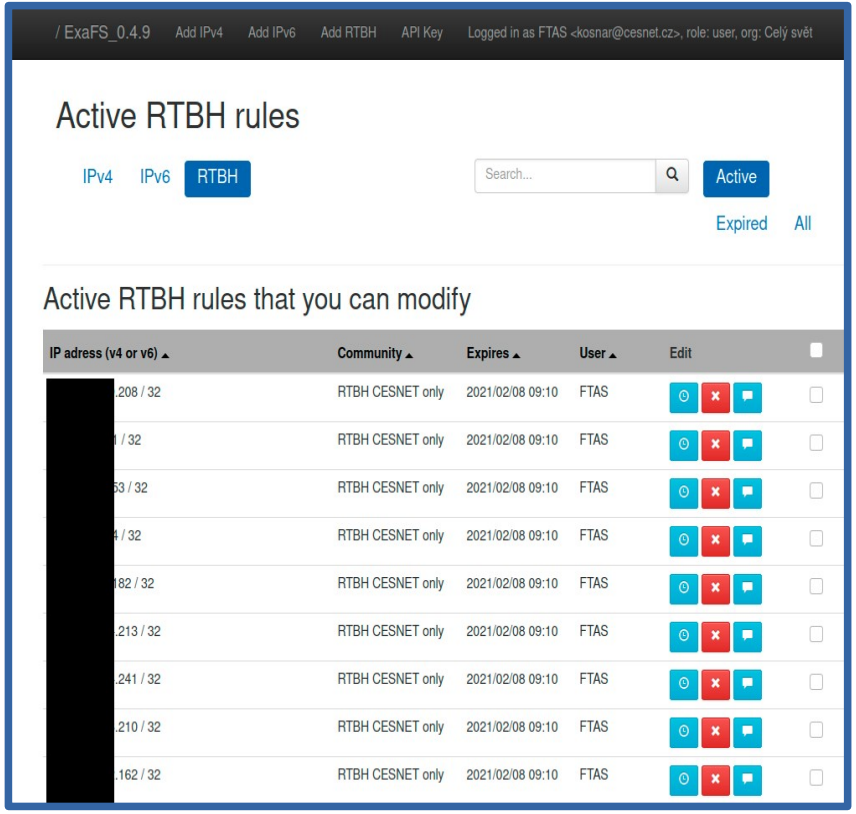
- **zamezit zahlcení**
  - **páteře**
  - **uživatelských přípojek**
  - ***externích propojení***
- **eliminovat nelegitimní provoz v síti**
- ošetřit/regulovat anomální jevy v síti
- ..
- pomoc uživatelům při řešení problémů v koncových sítích na úrovni transportu v síti e-infrastruktury
  - k dispozici nástroje pro analýzu a regulaci provozu (v e-infrastruktuře)
  - asistence při řešení konkrétních událostí

- Access listy
- Kontrola zdrojových adres
  - RPF checks, BCP-38
  - nativní funkce + filtry (access listy)
- RPKI (Resource Public Key Infrastructure)
  - validita oznamovaných prefixů
- Policing na perimetru sítě
  - nastavené profily pro specifický provoz (QoS)
  - typ provozu, granularita a limity
- DDoS protector

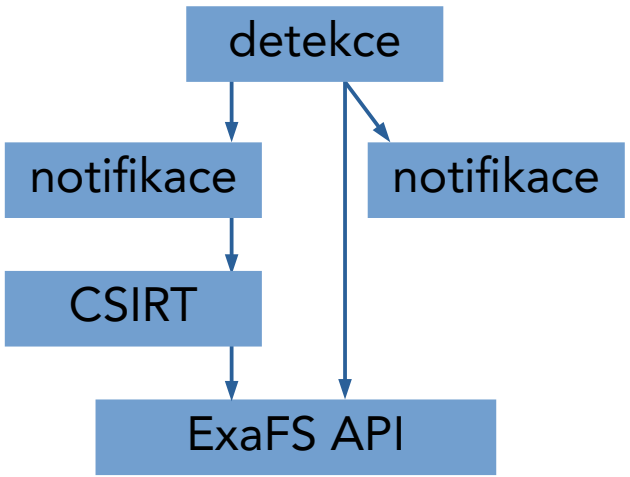
- Remotely Triggered Black Hole – RTBH
  - zahození provozu pro cílový prefix v předchozí (z hlediska směru přenosu) síti
- BGP FlowSpec
  - BGP rozšíření
  - jemnější rozhodování (na základě širší sady parametrů charakterizující datový tok)
    - prefixy, protokol, porty, ICMP (type, code), TCP flags, Pktlen, DSCP, Fragment encoding
  - aplikace pravidel pro regulaci
    - rate (vč, zahození), redirect, marking, action

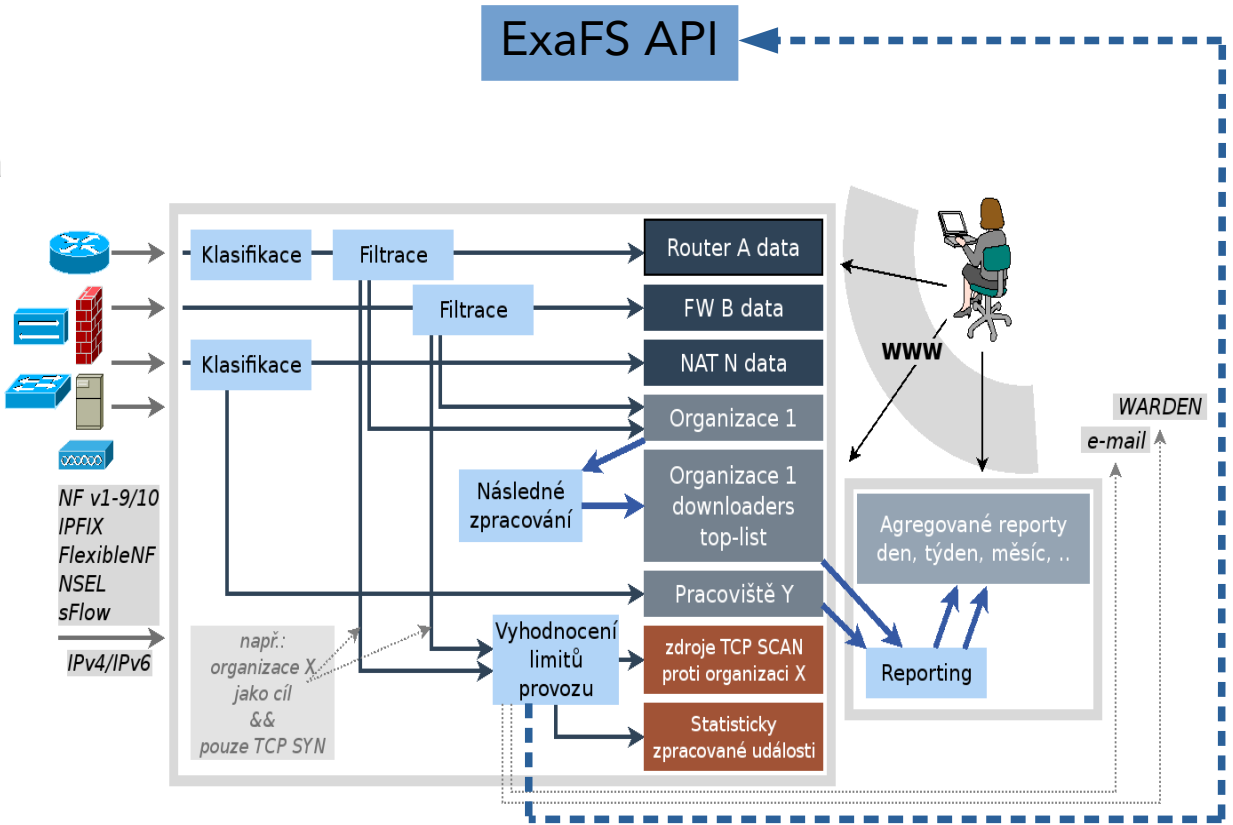
- usnadnění řízení RTBH + BGP FlowSpec (i směrování na DDoS protector)
- zpřístupnění uživatelské komunitě
- ExaFS
  - exaBGP
  - UI, API
  - k dispozici uživatelům
  - přístupová práva





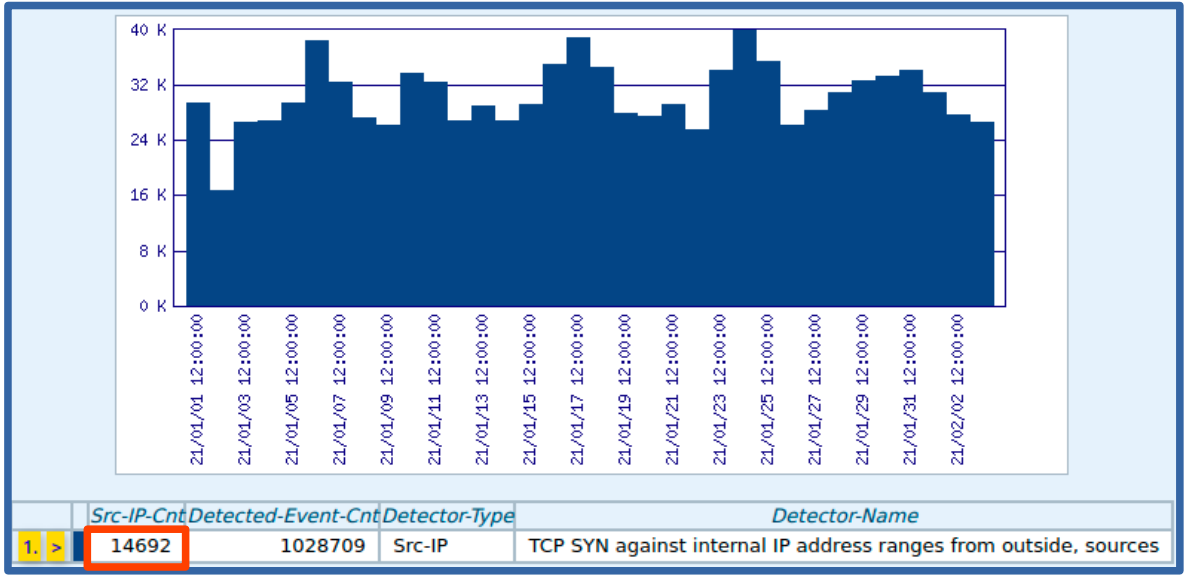
- plošný flow-based monitoring páteřní sítě
- FTAS
  - UI, API
  - 2020 nová detekční knihovna
  - přímé řízení ExaFS





- řízené čištění provozu ještě před vstupem do e-infrastruktury
  - realizováno ve spolupráci s poskytovatelem tranzitu
  - na základě specifické směrovací informace
    - přesměrování příslušného provozu již v síti Tier 1 operátora do čistící infrastruktury (potenciálně ošetří provoz, který by dorazil z více směrů)
    - návrat vyčištěného provozu specifickým kanálem
  - řízení ExaFS, FTAS+ExaFS

- vybrané detekované události
- sumarizace
- 1.1.-3.2. 2021



	Src-IP-Cnt	Detected-Event-Cnt	Detector-Type	Detector-Name
1. >	14692	1028709	Src-IP	TCP SYN against internal IP address ranges from outside, sources

o	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type	Detector-Name
1.	85735534	2615776	1028709	Src-IP	TCP SYN against internal IP address ranges from outside, sources
2.	74676050	0	1724	Src-IP	TCP SYN from internal IP address ranges
3.	201005	1103	1132	Src-IP	UDP (0, [redacted]) amplifiers external
4.	315554	241691	20	Dst-IP	IPv4 UDP (0, [redacted]) amplification targets internal
5.	32	0	4	Src-IP	UDP (0, [redacted]) amplifiers internal

- 11.-12. 2020 - amplifikační útoky – charakteristika jednoho z nich

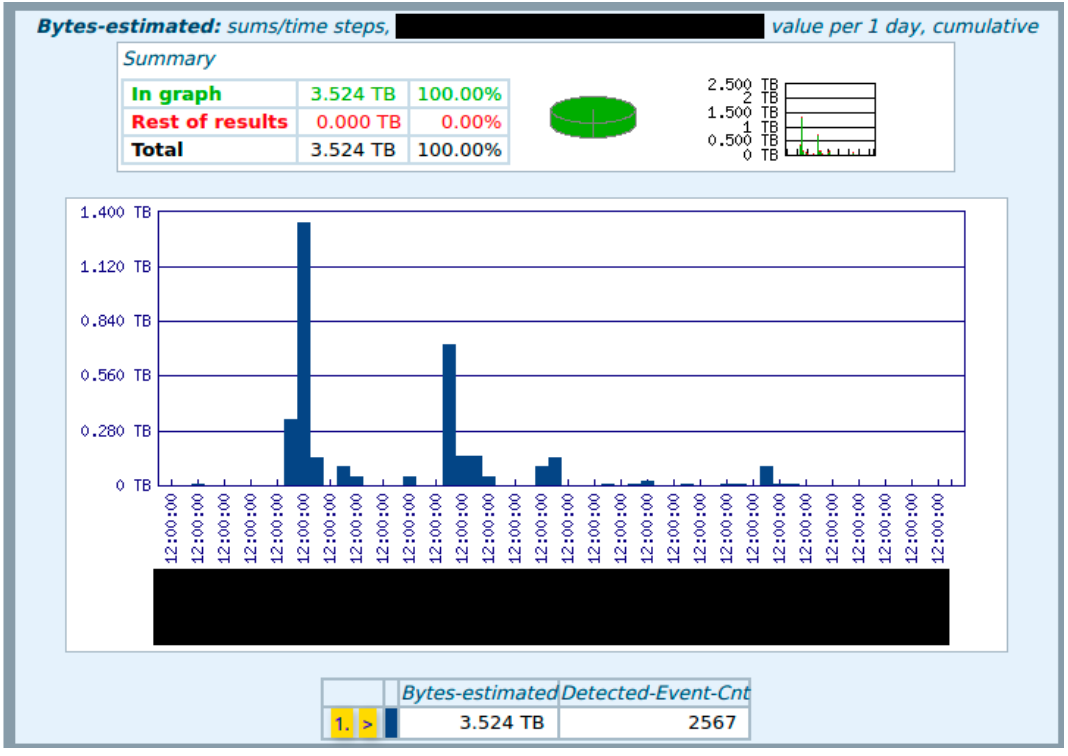
o	Flow-Direction	Protocol	Bytes-estimated	Pkts-estimated	Src-IP-Cnt
1.	ingress	udp (17)	1.537 TB	1.229 Gp	77560

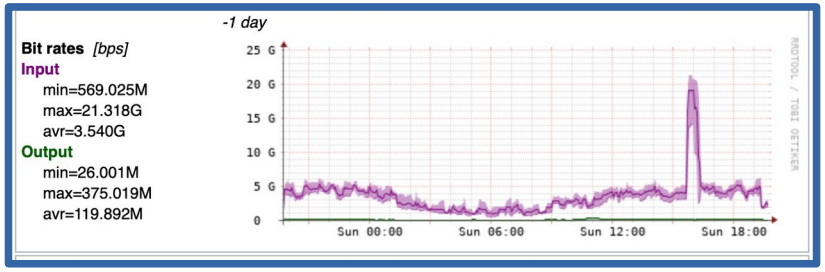
o	Flow-Direction	Protocol	Src-Port	Bytes-estimated	Pkts-estimated
1.	ingress	udp (17)	0	903.756 GB ~ 59.164%	771.205 Mp ~ 63.128%
2.	ingress	udp (17)	domain (53)	469.897 GB ~ 30.762%	347.841 Mp ~ 28.473%
3.	ingress	udp (17)	ldap (389)	153.896 GB ~ 10.075%	102.604 Mp ~ 8.399%

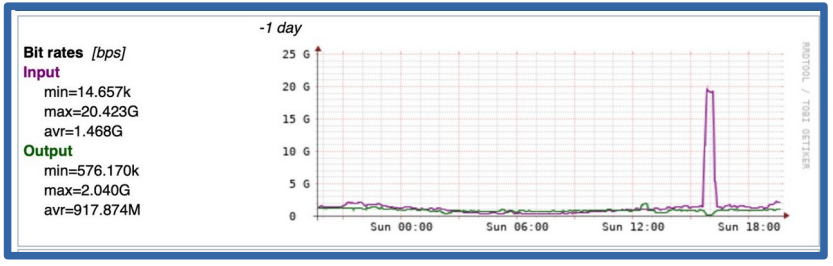
o	Flow-Direction	FWD-Status	Protocol	Bytes-estimated	Pkts-estimated
1.	ingress	Drop Policer	udp (17)	1.073 TB ~ 70.265%	860.402 Mp ~ 70.430%
2.	ingress	Forwarded	udp (17)	454.205 GB ~ 29.734%	361.231 Mp ~ 29.569%
3.	ingress	Drop RPF	udp (17)	5.619 MB ~ 0.000%	4.380 Kp ~ 0.000%
4.	ingress	Drop ACL drop	udp (17)	727.796 KB ~ 0.000%	12.436 Kp ~ 0.001%

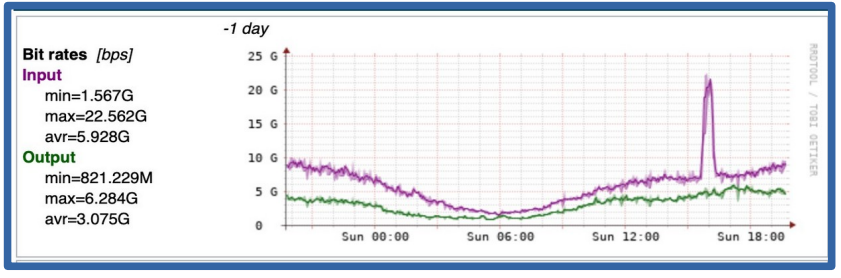
- *..nestačí, že se s tím uvnitř sítě umíme vypořádat..*

- 11.-12. 2020 - amplifikační útoky

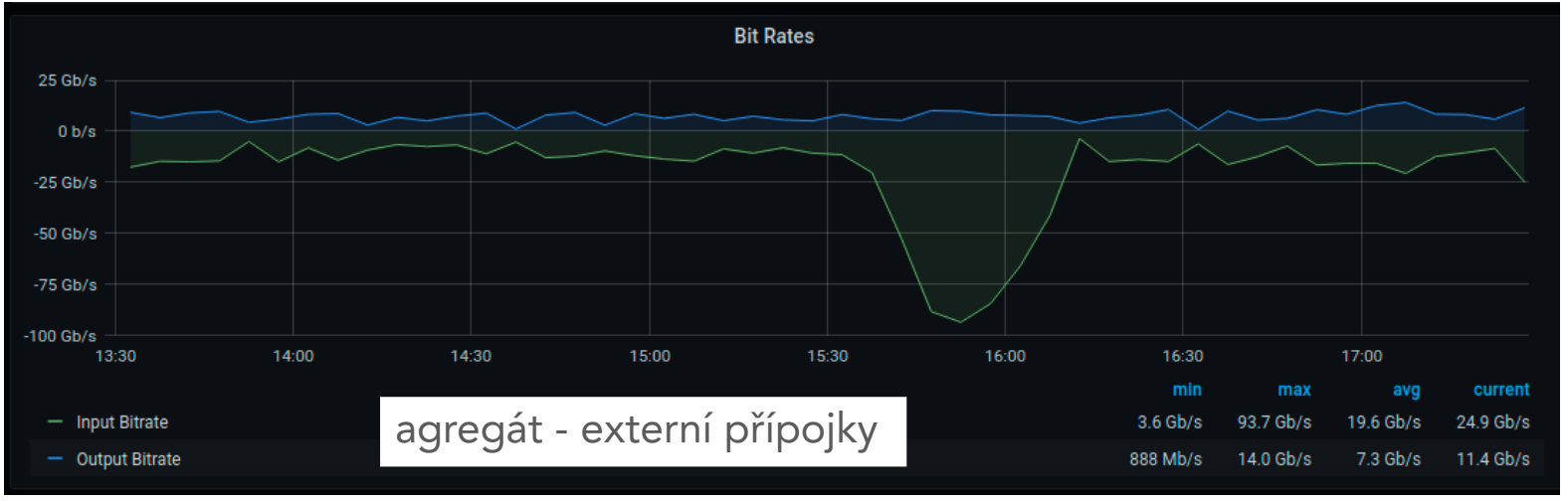








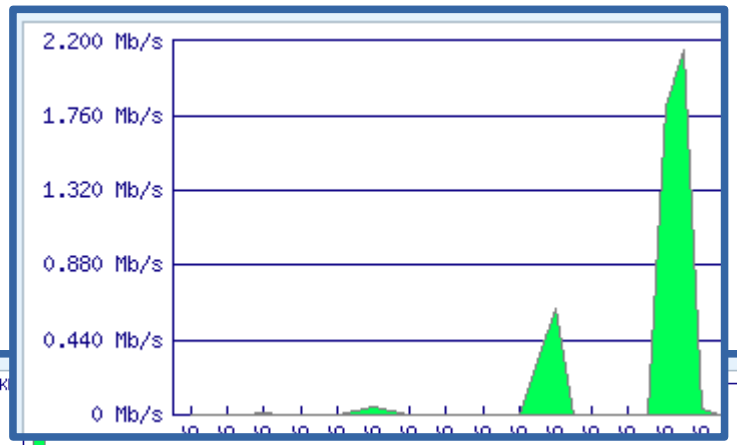
- 11.-12. 2020 - amplifikační útoky
- cca 120 Gb/s (část provozu zahozena v sítích externích partnerů)
- nutno řešit v „předchozích“ sítích

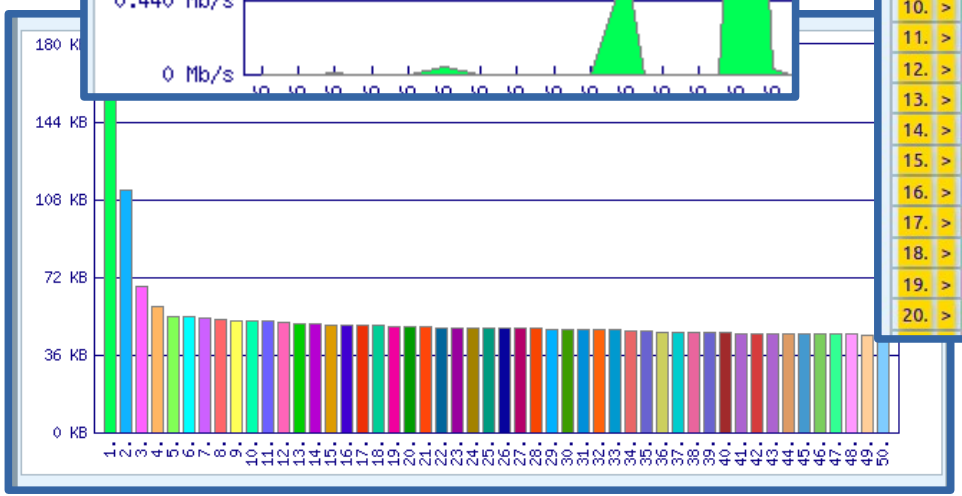


- útok neútok
  - *policing na perimetru je velmi užitečný, ale může mít i negativní dopad...*
  - *ne všechno je útok*
    - ..mezinárodní projekt, snaha o rychlý přenos
    - 65KB UDP paket je samozřejmě teoreticky možný
    - fragmentace to neurychlí (vs. ošetření v aplikaci)
    - doporučení - určitě do MTU, „mezinárodně“ radí ještě výrazně méně ;-)

o	Flow-Direction	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Bytes-measured	Pkts-measured	Avr-Pkt-Length
1.	egress	195.x.x.x	150.x.x.x	udp (17)	0	0	9.668 GB ~ 97.549%	6.519 Mp ~ 97.576%	1482.98
2.	egress	195.x.x.x	150.x.x.x	udp (17)	[redacted]		242.907 MB ~ 2.451%	161.938 Kp ~ 2.424%	1500

- trocha exotiky – součást série série útoků na koncovou síť





o	>	Flow-Direction	Protocol	Bytes-estimated	Avr-Pkt-Length
1.	>	egress	icmp (1)	168.862 KB ~ 2.650%	76.34
2.	>	egress	udp (17)	112.690 KB ~ 1.768%	132.89
3.	>	egress	tcp (6)	68.012 KB ~ 1.067%	83.35
4.	>	egress	54	58.304 KB ~ 0.915%	93.44
5.	>	egress	32	54.228 KB ~ 0.851%	95.81
6.	>	egress	40	53.998 KB ~ 0.847%	97.82
7.	>	egress	13	53.218 KB ~ 0.835%	93.36
8.	>	egress	116	52.508 KB ~ 0.824%	96.88
9.	>	egress	iso-tp4 (29)	51.936 KB ~ 0.815%	96.90
10.	>	egress	st (5)	51.674 KB ~ 0.811%	98.99
11.	>	egress	skip (57)	51.644 KB ~ 0.810%	96.71
12.	>	egress	143	51.354 KB ~ 0.806%	102.71
13.	>	egress	95	50.658 KB ~ 0.795%	97.42
14.	>	egress	18	50.546 KB ~ 0.793%	98.72
15.	>	egress	107	50.004 KB ~ 0.785%	102.47
16.	>	egress	56	49.916 KB ~ 0.783%	96.74
17.	>	egress	76	49.642 KB ~ 0.779%	91.25
18.	>	egress	rspf (73)	49.634 KB ~ 0.779%	95.08
19.	>	egress	wesp (141)	49.460 KB ~ 0.776%	97.75
20.	>	egress	65	49.240 KB ~ 0.773%	96.93

21.	>	egress	25
22.	>	egress	131
		ess	117
		ess	105
		ess	53
		ess	14
		ess	123
		ess	121
		ess	90
		ess	77
		ess	dccp (33)
		ess	42
		ess	67
		ess	113
		ess	hmp (20)
		ess	82
		ess	92
		ess	99
		ess	104
		ess	61
		ess	eigrp (88)
		ess	pim (103)
		ess	mobility-header (135)
		ess	esp (50)
		ess	hip (139)
46.	>	egress	idpr-cmtp (38)
47.	>	egress	19
48.	>	egress	shim6 (140)
49.	>	egress	vmtp (81)
50.	>	egress	101

limity

- **obecně má řešení útoků a anomálií na úrovni páteře jasné limity**
  - jde pouze o malou část celého přenosového řetězce
  - možnosti dány architekturou sítě, logickým nastavením
  - rozhodování se odvíjí od informací o transportu
  - schopnost identifikace detailu v celkovém objemu agregovaného provozu (~ hledání v „bílém“ šumu)
    - mohou pomoci oddělené, danému účelu dedikované celky (např. aktivita hSOC)
  - schopnost minimalizovat riziko false positives při „tvrdé“ regulaci
  - volba strategie pro události se zdrojem uvnitř AS vs. vně AS

- *poděkování správcům koncových sítí za spolupráci*
- *omluva za to, co se občas nepovede..*

- **..to podstatné je v koncové síti**
  - hraniční prvek/síťové zabezpečení
  - vnitřní síť - architektura, segmentace, řízení toků
  - ošetření koncových uzlů
  - systematická správa a péče o celou infrastrukturu
  - práce s uživateli

- *...bezpečnost nelze „outsourcovat“*

perličky na závěr

- *Vřelé díky všem*
  - *za věcný popis problému (včetně přesného časového vymezení) – je to mravenčí práce, kterou málokdo docení, ale bez ní bychom plácali jen prázdnou slámu…*
  - *za dobře zvolený komunikační kanál (CSIRT, ...)*
- pod tlakem si občas neuvědomíme, co chceme a komu a jak si o to říkáme ;-)
  - Dobrý den, děláme audit sítí organizací X a Y ..a nemůžeme to tam protlačit – můžete dát tyto naše IP do vašeho white-listu..
  - Dobrý den, neblokujete něco ? Naši uživatelé si občas stěžují, že se nemohou připojit k naší službě... Můžete se na to podívat..?
  - Dobrý den, mohli byste vystavit seznam blokovaných IP na web ? Ladím apku u klienta a chci mít jistotu, že to nezahazujete..


cesnet
Díky za pozornost.