cesnet

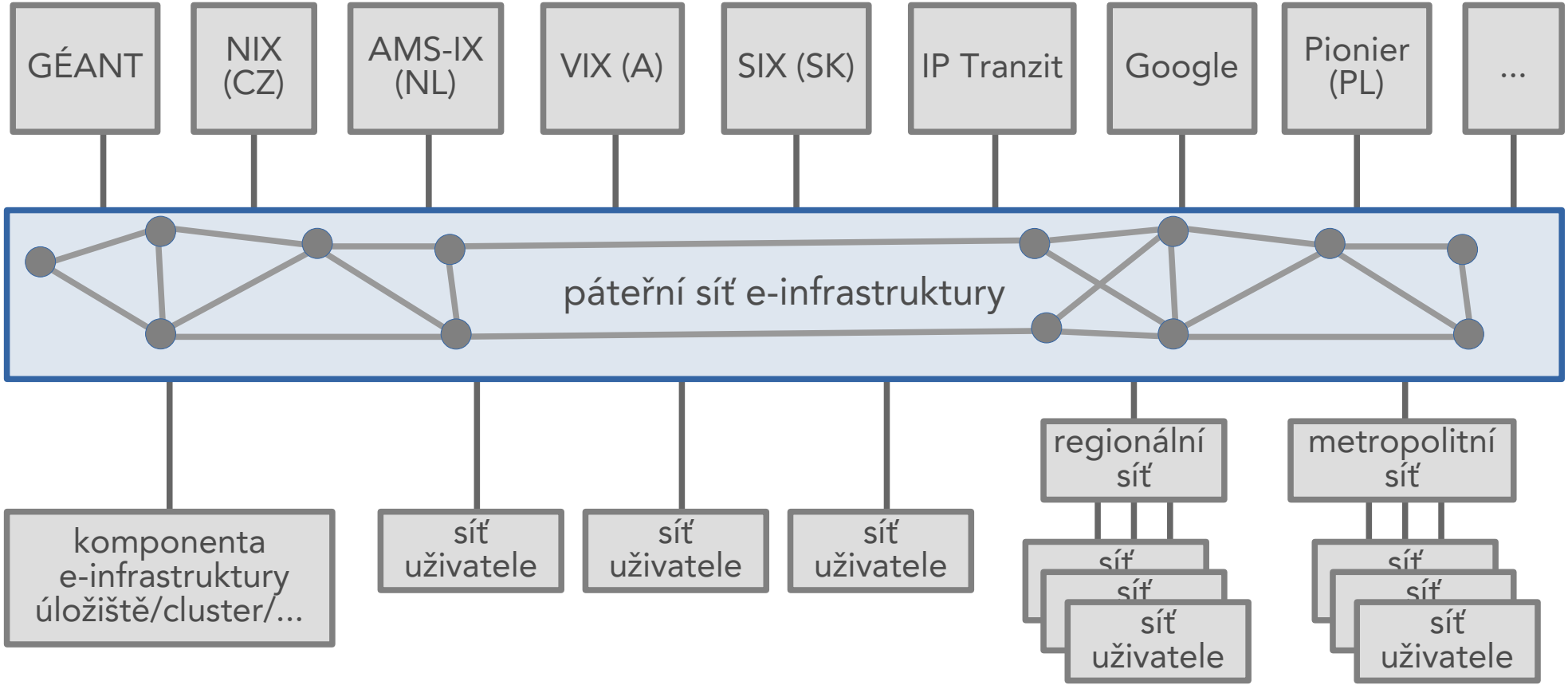
Bezpečnost na úrovni síťového transportu v e-infrastruktuře CESNET

Tomáš Košňar
CESNET

AV ČR
1. 2. 2023

cesnet

základní síťové schéma

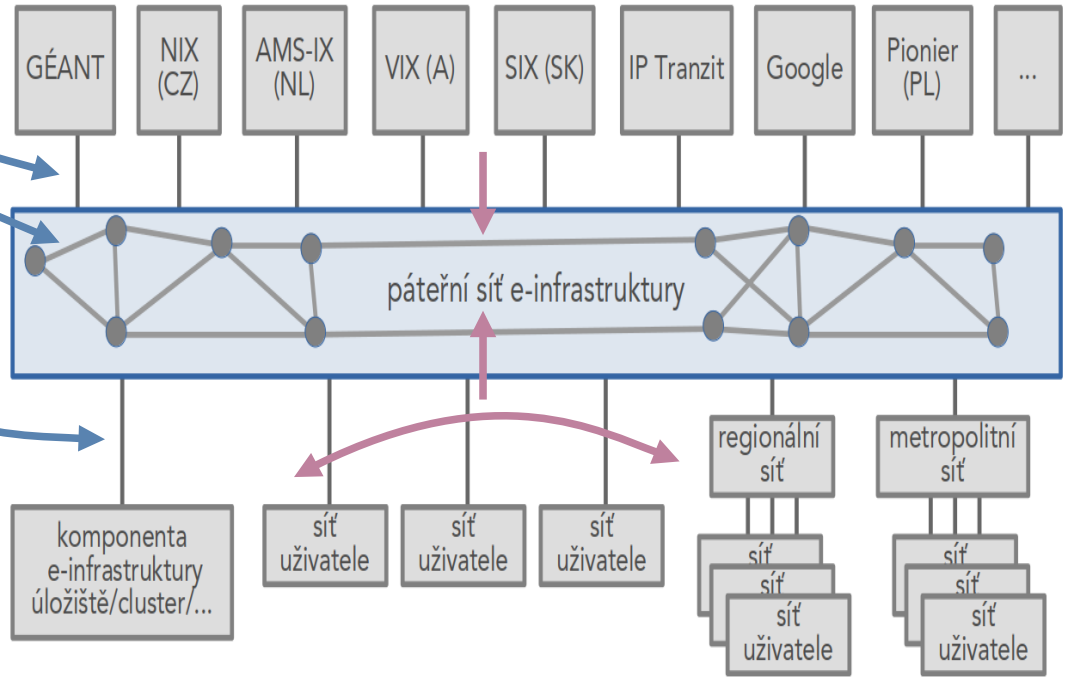


cesnet

k řešení v oblasti bezpečnosti

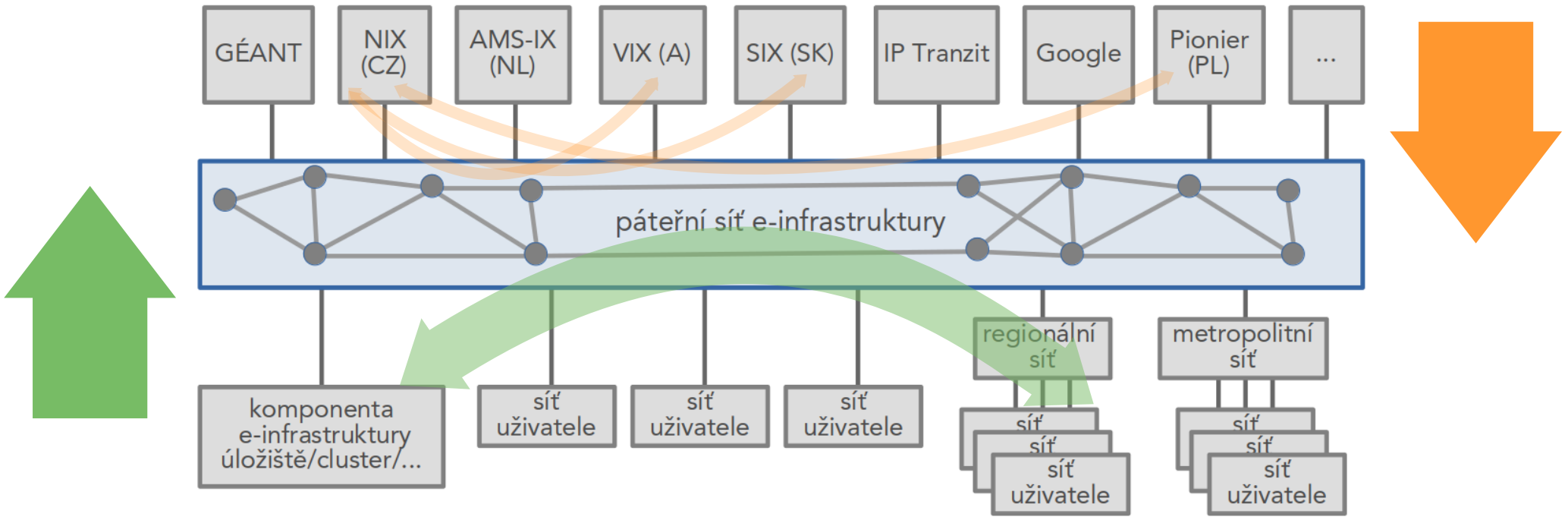
- zahlcení externích propojení
- zahlcení páteře
- zahlcení uživatelských přípojek
- nelegitimní provoz
- anomální jevy v provozu
  - vztah k cílům/zdrojům
  - v sítích uživatelů / v externích sítích

- ošetření v e-infrastruktuře
  - automatické
  - semi-automatické, ruční na základě analýzy (správci sítě, CSIRT)
  - samoobslužné ošetření uživateli
    - nástroje v e-infrastruktuře
    - asistence



bezpečnostní strategie vzhledem k původu událostí

- **z vnějších sítí → automatické**/semi-automatické **ošetření**/regulace provozu
- **z vnitřních sítí → semi-automatické ošetření**, analýza, komunikace s uživateli, regulace provoxu
- **extrémní případy ?**



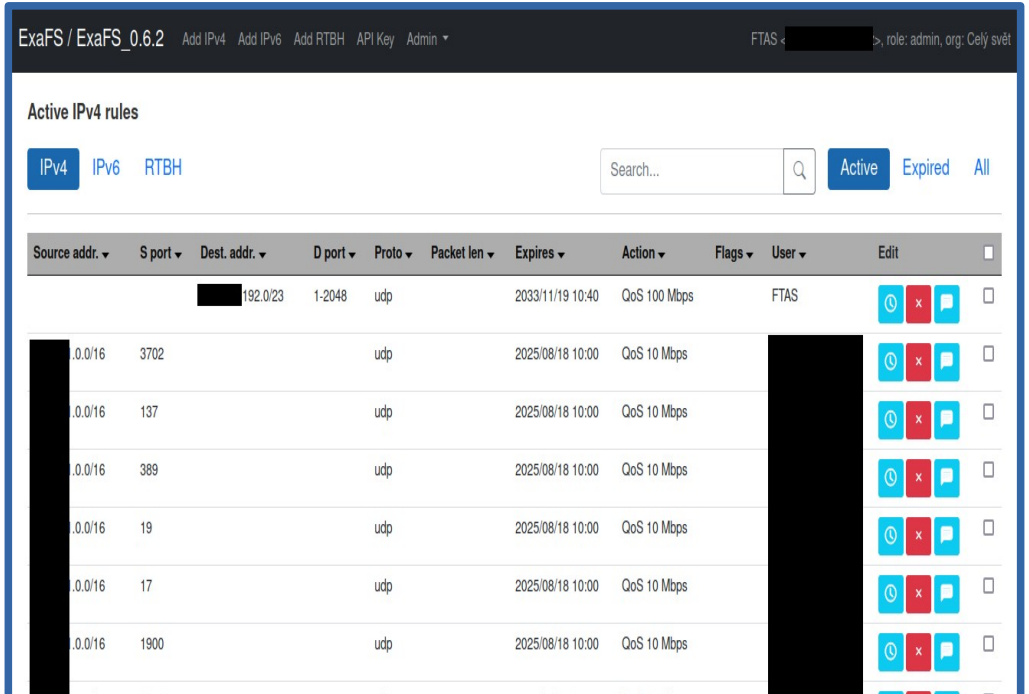
bezpečnostní mechanismy

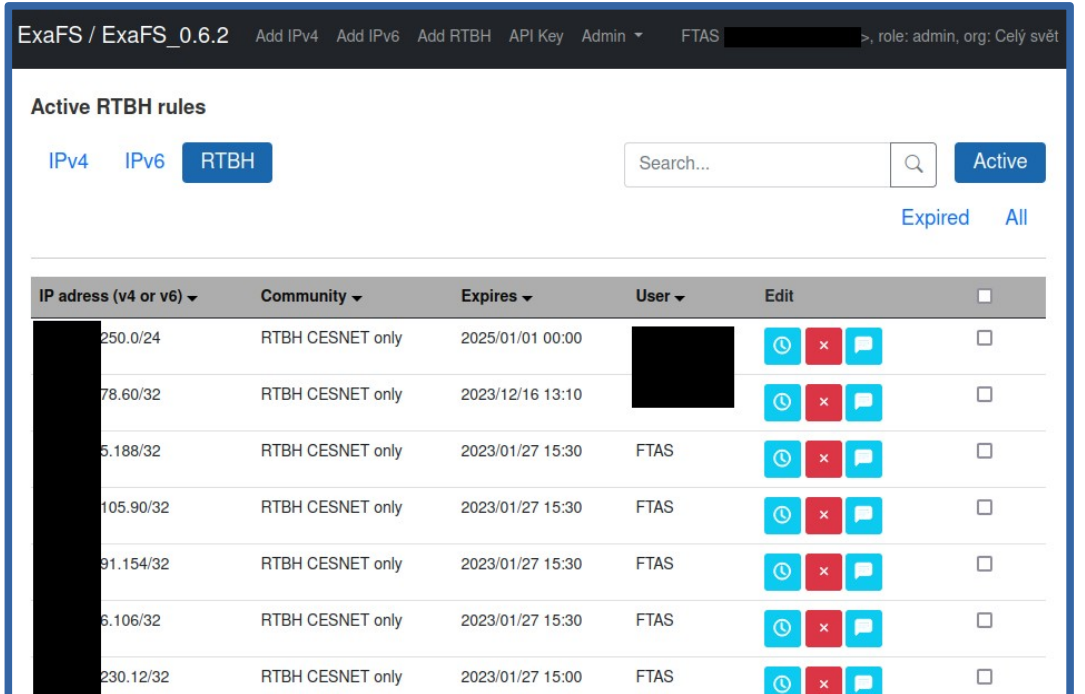
- **nastavení sítě, permanentní mechanismy**
  - ACL (Access Lists)
  - **Kontrola zdrojových adres** (Reverse Path Forwarding kontroly, BCP-38)
  - **RPKI** (Resource Public Key Infrastructure) - validita oznamovaných prefixů
  - **Policing na perimetru sítě (QoS)** - profily pro specifický provoz
- **ad-hoc/dynamicky řízené mechanismy**
  - **RTBH** (Remotely Triggered Black Hole)
  - *DoS protector*
  - **BGP FlowSpec** (rozšířený Border Gateway Protocol)
  - **vzdálené čištění provozu** (řízené na bázi přesměrování)

cesnet

nástroj pro centrální řízení

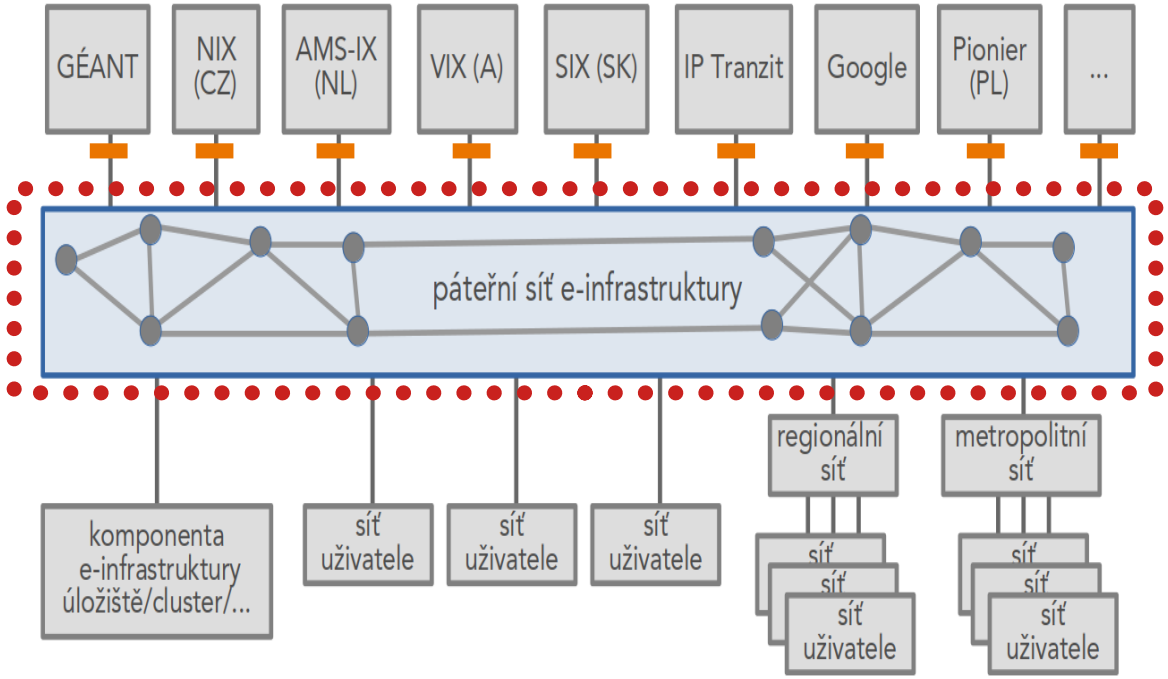
- **ExaFS - jednotný přístup k řízení/regulaci provozu**
  - ExaBGP, UI/API, školení před přístupněním, práva k vlastním prefixům
  - RTBH, BGP FlowSpec, vzdálené čištění provozu, *DoS protector*

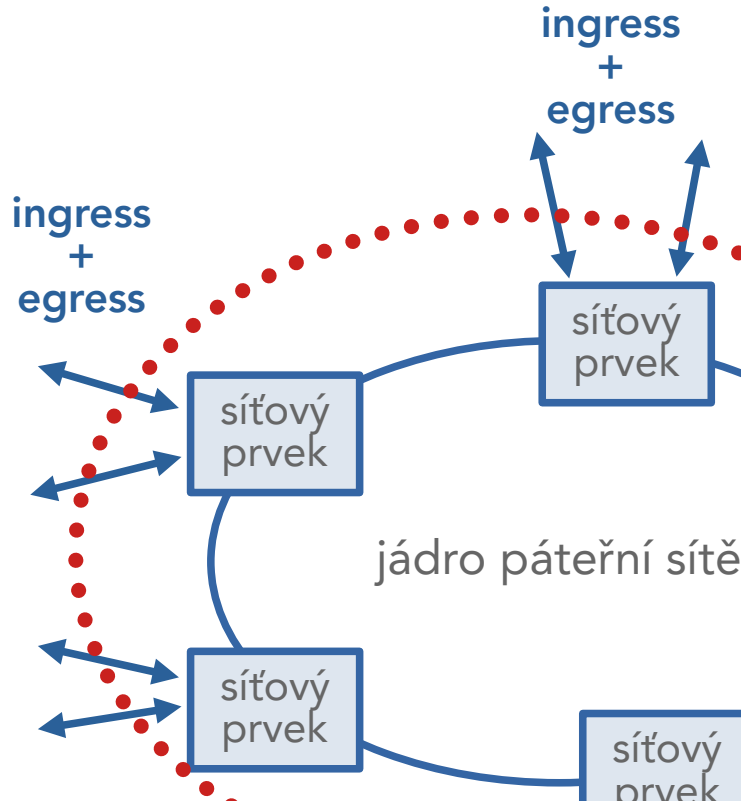




plošný monitoring provozu

- permanentní, na bázi toků (flow-based, netflow, IPFIX)
  - páteřní směrovače → externí a klientská rozhraní, ingress+egress
  - *sondy na externích linkách (on-demand)*





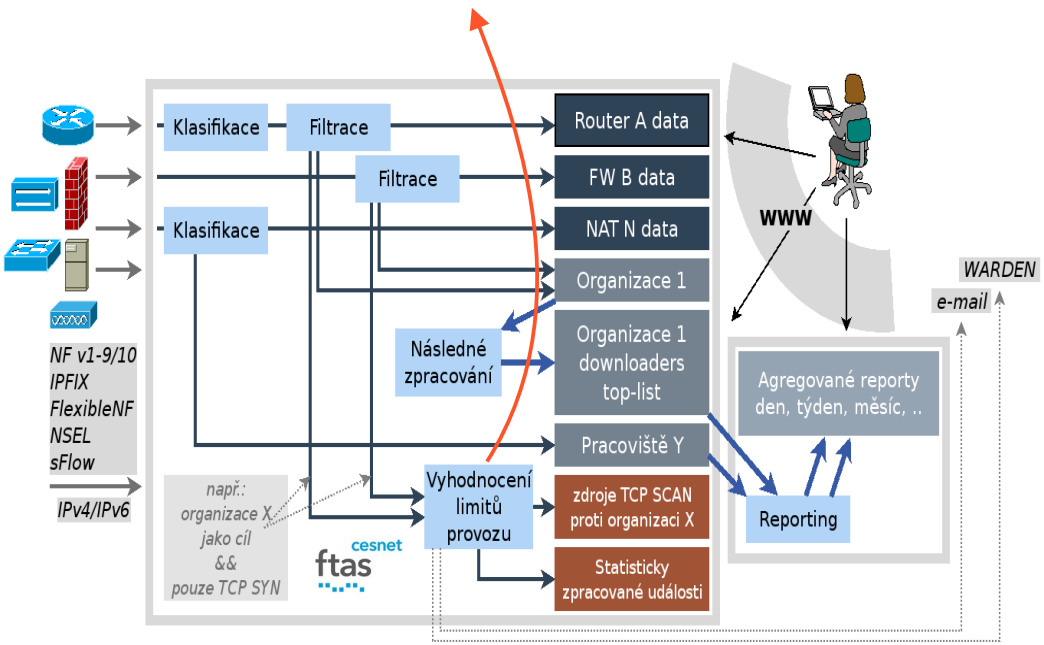
- ukázka vypovídací hodnoty dat z páteřního směrovače

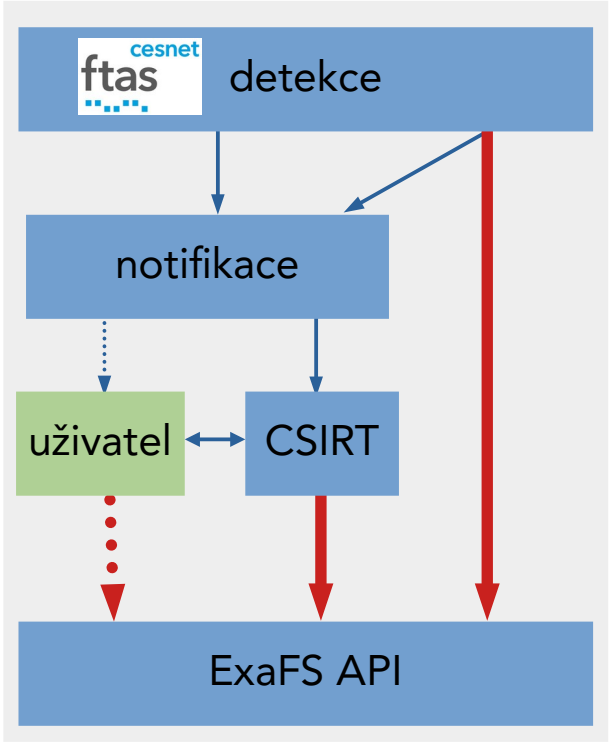
Flow-Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Ingress-VRFID	Egress-VRFID
ingress	Forwarded	2001:718:1:1f:50:x:x:x	2a01:430:17d:0:0:x:x:x	tcp (6)	https (443)	55096	90974	183	0x60000000	0x60000000
ingress	Forwarded	2001:718:1:1f:50:x:x:x	2a00:11c0:4:429:0:x:x:x	tcp (6)	https (443)	49814	90974	183	0x60000000	0x60000000
ingress	Forwarded	2001:718:1:1f:50:x:x:x	2a01:430:17d:0:0:x:x:x	tcp (6)	https (443)	40228	90974	183	0x60000000	0x60000000
ingress	Forwarded	2001:718:1:1f:50:x:x:x	2a00:11c0:4:429:0:x:x:x	tcp (6)	https (443)	37696	90974	183	0x60000000	0x60000000
ingress	Forwarded	2001:718:1:1f:50:x:x:x	2a00:11c0:4:429:0:x:x:x	tcp (6)	https (443)	57626	90974	183	0x60000000	0x60000000
egress	Forwarded not Fragmented	78.128.211.x	79.110.73.x	tcp (6)	https (443)	33953	90974	90553	0x60000000	0x60000000
ingress	Forwarded	78.128.211.x	79.110.73.x	tcp (6)	https (443)	33953	90974	90553	0x60000000	0x60000000
ingress	Forwarded	78.128.211.x	195.178.64.x	tcp (6)	ssh (22)	40680	90974	183	0x60000000	0x60000000
ingress	Forwarded	78.128.211.x	195.178.64.x	tcp (6)	ssh (22)	40694	90974	183	0x60000000	0x60000000

Src/Prev-AS	Dst/Next-AS	Src-Bitmask	Dst-Bitmask	TOS-flags	TCP-flags	Nexthop	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated
AS65089	AS24971	64	32	00000000	push(8), ack(16)	0:0:0:0:0:x:x:x	22/05/25 12:55:00.655	22/05/25 12:55:01.009	259.153 KB	5.183 MB	173.000 p	3.460 Kp
AS65089	AS42473	64	48	00000000	push(8), ack(16)	0:0:0:0:0:x:x:x	22/05/25 12:55:00.573	22/05/25 12:55:06.016	246.613 KB	4.932 MB	166.000 p	3.320 Kp
AS65089	AS24971	64	32	00000000	push(8), ack(16)	0:0:0:0:0:x:x:x	22/05/25 12:55:05.809	22/05/25 12:55:06.139	237.759 KB	4.755 MB	159.000 p	3.180 Kp
AS65089	AS42473	64	48	00000000	syn(2), push(8), ack(16)	0:0:0:0:0:x:x:x	22/05/25 12:50:11.889	22/05/25 12:50:12.296	219.945 KB	4.399 MB	149.000 p	2.980 Kp
AS65089	AS42473	64	48	00000000	fin(1), push(8), ack(16)	0:0:0:0:0:x:x:x	22/05/25 12:55:06.589	22/05/25 12:55:13.038	211.282 KB	4.226 MB	144.000 p	2.880 Kp
AS65089	AS50245	24	20	00000000	ack(16)	80.249.214.x	22/05/25 12:47:02.057	22/05/25 12:47:02.693	155.600 KB	3.112 MB	104.000 p	2.080 Kp
AS65089	AS50245	24	20	00000000	syn(2), ack(16)	80.249.214.x	22/05/25 12:47:01.488	22/05/25 12:47:02.791	148.756 KB	2.975 MB	101.000 p	2.020 Kp
AS65089		24	28	00001000	push(8), ack(16)	195.113.235.x	22/05/25 12:46:14.512	22/05/25 12:46:24.618	99.512 KB	1.990 MB	1.319 Kp	26.380 Kp
AS65089		24	28	00001000	fin(1), push(8), ack(16)	195.113.235.x	22/05/25 12:47:02.366	22/05/25 12:47:12.351	98.848 KB	1.977 MB	1.300 Kp	26.000 Kp
AS65089		24	28	00001000	push(8), ack(16)	195.113.235.x	22/05/25 12:52:08.451	22/05/25 12:52:18.992	98.536 KB	1.971 MB	1.312 Kp	26.240 Kp

zpracování informací z monitoringu
schéma řízení obrany

- FTAS – zpracování, uchování a zpřístupnění provozních informací na bázi toků
- UI, API
- funkce pro konfiguraci detektorů
- přímé řízení exaFS API

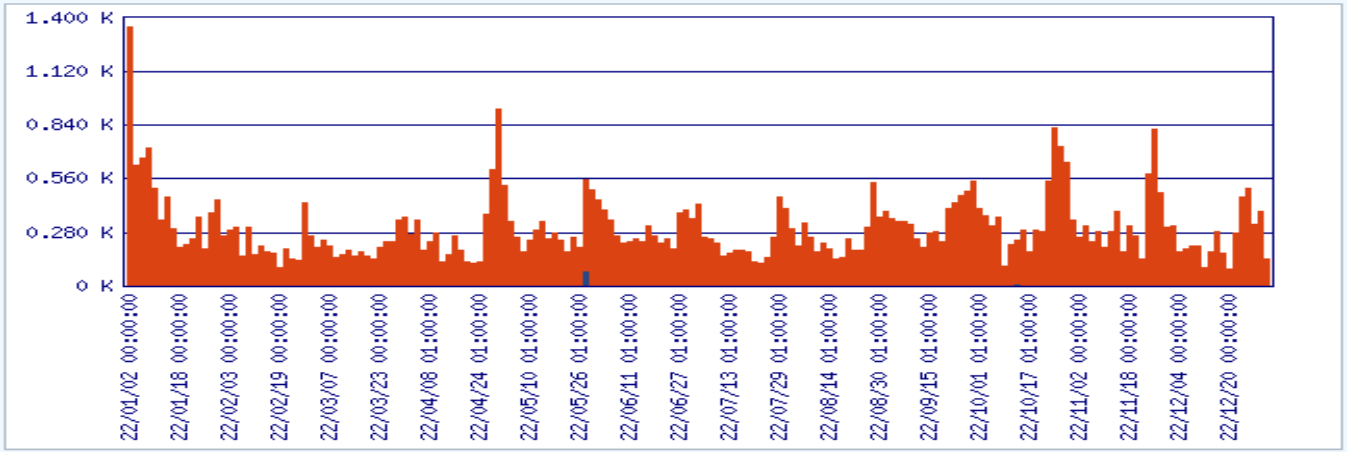




typické automaticky řešené útoky/anomálie

- agresivní objemově orientovaný (odraz/amplifikace) na bázi UDP
- TCP/SYN útoky proti vybraným cílům
- plošné/vertikální/horizontální TCP skenování, cílené plošné UDP skenování

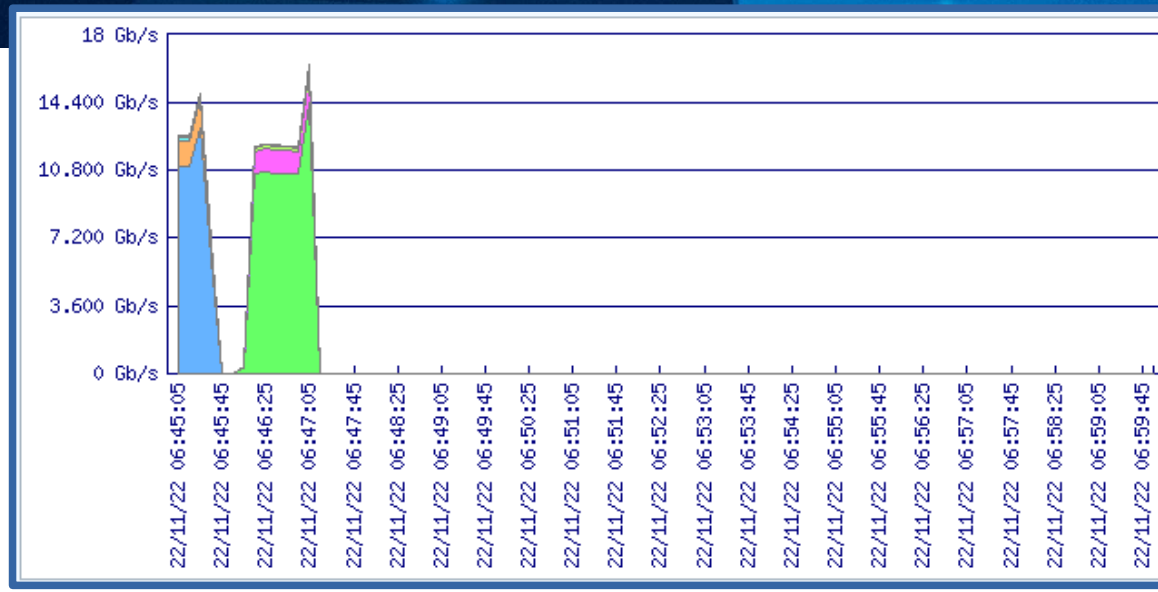
Detected-Event-Cnt: *sums/time steps, 22/01/01 00:00:00-22/12/31 23:59:00, value per 2 days, cumulative*



	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Dst-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
1. >	725.163 GB	901.506 Mp	1	205	2133373	529294	418	Dst-IP
2. >	362.208 GB	4.223 Gp	28321	1	43140539	1103807	54878	Src-IP

ukázka automaticky ošetřeného útoku

- **odraz/amplifikace UDP/ntp vůči 2 cílům**
- policing na perimetru (viz. podíl zahozeného provozu)
- kardinalita, počet „zrcadel“, počet cílových portů
- rozložení mezi externí boxy
- detekce → vzdálené čištění → ztráta visibility

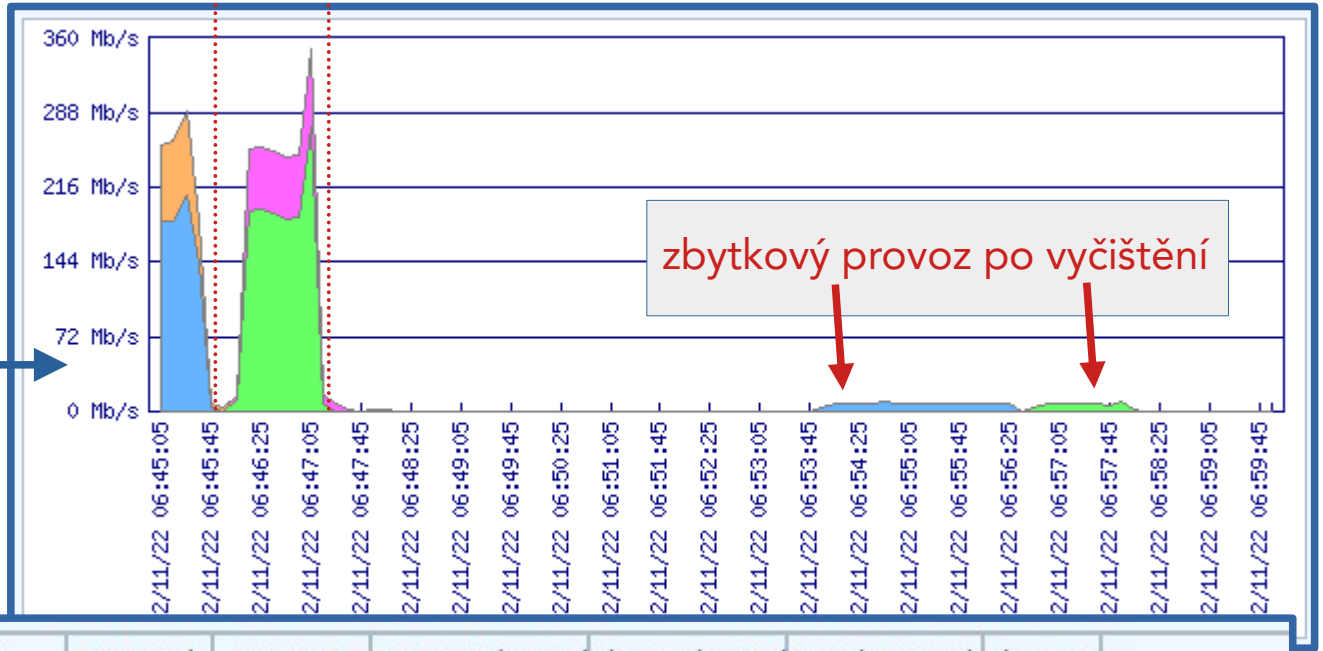


o	Flow-Direction	FWD-Status	Dst-IP	Protocol	Src-Port	Flow-Start [CET]	Flow-End [CET]	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt	Flow-Data-Sc
1.	ingress	Drop Policer	147.251.5.x	udp (17)	ntp (123)	22/11/22 06:46:09.306	22/11/22 06:47:09.583	84.921 GB ~ 51.827%	184.018 Mp ~ 51.938%	908	20	461.48	106621 ~ 42.974%	Praha 1: R14
2.	ingress	Drop Policer	147.251.14.x	udp (17)	ntp (123)	22/11/22 06:44:49.999	22/11/22 06:46:11.472	58.374 GB ~ 35.625%	126.172 Mp ~ 35.611%	921	20	462.65	70668 ~ 28.483%	Praha 1: R14
3.	ingress	Drop Policer	147.251.5.x	udp (17)	ntp (123)	22/11/22 06:46:08.974	22/11/22 06:47:09.647	9.719 GB ~ 5.931%	20.855 Mp ~ 5.886%	91	20	466.02	11312 ~ 4.559%	Praha 2: R13
4.	ingress	Drop Policer	147.251.14.x	udp (17)	ntp (123)	22/11/22 06:44:50.078	22/11/22 06:45:33.884	7.170 GB ~ 4.376%	15.376 Mp ~ 4.340%	89	20	466.33	6998 ~ 2.821%	Praha 2: R13
5.	ingress	Forwarded	147.251.5.x	udp (17)	ntp (123)	22/11/22 06:46:08.715	22/11/22 06:58:01.428	1.635 GB ~ 0.998%	3.508 Mp ~ 0.990%	93	20	466.07	9761 ~ 3.934%	Praha 2: R13
6.	ingress	Forwarded	147.251.14.x	udp (17)	ntp (123)	22/11/22 06:44:50.025	22/11/22 06:56:25.777	1.155 GB ~ 0.705%	2.476 Mp ~ 0.699%	90	20	466.43	6112 ~ 2.463%	Praha 2: R13
7.	ingress	Forwarded	147.251.5.x	udp (17)	ntp (123)	22/11/22 06:46:09.283	22/11/22 06:48:09.199	500.634 MB ~ 0.306%	1.080 Mp ~ 0.305%	901	20	463.46	23456 ~ 9.454%	Praha 1: R14
8.	ingress	Forwarded	147.251.14.x	udp (17)	ntp (123)	22/11/22 06:44:50.076	22/11/22 06:46:09.283	379.711 MB ~ 0.232%	815.940 Kp ~ 0.230%	878	20	465.37	13189 ~ 5.312%	Praha 1: R14

o	Protocol	Src-Port	Flow-Start [CET]	Flow-End [CET]	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
1.	udp (17)	ntp (123)	22/11/22 06:44:49.999	22/11/22 06:58:01.428	163.855 GB ~100.000%	354.301 Mp ~100.000%	1015	40	462.47	248108 ~1

ukázka automaticky ošetřeného útoku

- **odraz/amplifikace UDP/ntp vůči 2 cílům**
- ..vzdálené čištění
- zbytkový provoz ?
  - pouze to, co jsme pustili dál



< o	Flow-Direction	FWD-Status	Dst-IP	Protocol	Src-Port	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt	
5. >	ingress	Forwarded	147.251.5.x	udp (17)	ntp (123)	1.635 GB	3.508 Mp	466.07	9761	Praha 2: R13
6. >	ingress	Forwarded	147.251.14.x	udp (17)	ntp (123)	1.155 GB	2.476 Mp	466.43	6112	Praha 2: R13
7. >	ingress	Forwarded	147.251.5.x	udp (17)	ntp (123)	500.634 MB	1.080 Mp	463.46	23456	Praha 1: R14
8. >	ingress	Forwarded	147.251.14.x	udp (17)	ntp (123)	379.711 MB	815.940 Kp	465.37	13180	Praha 1: R14

závěry

- **(automatické) řešení útoků a anomálií na úrovni páteře**
  - architektura sítě, strategie doručování dat, nasazené nástroje
  - typ provozu (výzkumné aplikace !!! vs. běžný uživatelský provoz), míra agregace
  - identifikace provozních detailů → informace o transportu nikoli o obsahu !!!
  - úroveň citlivosti vs. riziko false-positives
- **analogické ošetření/péče v koncové síti**
  - zabezpečení perimetru, citlivých částí sítě
  - vnitřní síť - architektura, segmentace, řízení toků
  - ošetření koncových uzlů
  - důsledná a systematická správa a péče o infrastrukturu *...personál vs. nákup řešení..?*
  - *...práce s uživateli, práce s uživateli, práce s uživateli, práce s uživateli, práce s uživateli…?*


cesnet
Díky za pozornost.