cesnet

FTAS “as a service”

Tomáš Košňar
CESNET

Seminář o bezpečnosti sítí a služeb
7. 2. 2023

cesnet

motivace

```
# Flow-Direction;FWD-Status;Src-IP;Dst-IP;Protocol;Src-Port;Dst-Port;Src-ifIndex;Dst-ifIndex;Ingress-VRFID;Egress-VRFID;Src/Prev-AS;Dst/Next-AS;Src-Bitmask;Ds
estimated;Avr-Pkt-Length
# flow_direction;forwarding_status;src_ip;dst_ip;proto;src_port;dst_port;src_if;dst_if;src_vrfid;dst_vrfid;src_as;dst_as;src_mask;dst_mask;tos;tcp_flags;statis
egress;Forwarded;188.120.x.x;78.128.x.x;tcp (6);2809;http (80);157;195;0x60000000;0x60000000;AS49985;AS65089;19;24;00000000;push(8), ack(16);8380;70;119.71
ingress;Forwarded;78.128.x.x;217.11.x.x;icmp (1);Echo-reply (0);Echo-reply (0);195;157;0x60000000;0x60000000;AS65089;AS15685;24;24;00000000;;52800;550;96
egress;Forwarded;2001:67c:x:e100:x:x:x:x;2001:718:x:1f:x:x:x:x;ipv6-icmp (58);0;128;157;195;0x60000000;0x60000000;AS197451;;46;64;00000000;;356320;340;1048
egress;Forwarded;88.102.x.x;78.128.x.x;icmp (1);Echo-reply (0);Echo-reply (0);157;195;0x60000000;0x60000000;AS5610;AS65089;16;24;10000000;;113560;1340;84.75
ingress;Forwarded;78.128.x.x;88.101.x.x;icmp (1);Echo-reply (0);Echo-reply (0);195;157;0x60000000;0x60000000;AS65089;AS5610;24;15;10000000;;31200;520;60
egress;Forwarded;185.191.x.x                                                                                                                    0;fin(1), push(8), ack(16);10630
ingress;Forwarded;78.128.x.x                                                                                                                    00000000;;60600;1010;60
egress;Forwarded;194.50.x.x;                                                                                                                    4;24;00000000;;41600;800;52
ingress;Forwarded;78.128.x.x                                                                                                                    0;push(8), ack(16);900830;650;13
ingress;Forwarded;78.128.x.x                                                                                                                    24;22;00000000;;3360;40;84
ingress;Forwarded;78.128.x.x                                                                                                                    );syn(2), push(8), ack(16);8760;2
egress;Forwarded;66.249.x.x;                                                                                                                    ;ack(16);520;10;52
ingress;Forwarded;2001:718:x                                                                                                                    4;32;00000000;;126880;1220;104
egress;Forwarded;134.158.x.x                                                                                                                    fin(1), rst(4), push(8), ack(16);
egress;Forwarded;5.59.x.x;78                                                                                                                    push(8), ack(16);1800;10;180
egress;Forwarded;109.164.x.x                                                                                                                    );push(8), ack(16);710;10;71
egress;Forwarded;212.119.x.x                                                                                                                    ;22;24;00000000;;524160;800;655.2
egress;Forwarded;31.31.x.x;7                                                                                                                    ack(16);800;20;40
ingress;Forwarded;78.128.x.x                                                                                                                    4;16;10000000;;107720;1280;84.16
egress;Forwarded;92.62.x.x;7                                                                                                                    k(16);520;10;52
ingress;Forwarded;78.128.x.x                                                                                                                    ;fin(1), ack(16);15840;30;528
egress;Forwarded;217.11.x.x;                                                                                                                    4;24;00000000;;47040;490;96
ingress;Forwarded;35.204.x.x                                                                                                                    0;ack(16);520;10;52
egress;Forwarded;139.28.x.x;                                                                                                                    );rst(4), ack(16);400;10;40
ingress;Forwarded;78.128.x.x                                                                                                                    fin(1), ack(16);520;10;52
egress;Forwarded;195.113.x.x;                                                                                                                   0000000;;63600;1060;60
egress;Forwarded;2a00:1028:x:25ee:x:x:x:x;2001:718:x:1f:x:x:x:x;tcp (6);60843;https (443);157;195;0x60000000;0x60000000;AS5610;;32;64;10000000;syn(2), ack(16)
ingress;Forwarded;78.128.x.x;137.189.x.x;tcp (6);https (443);60378;195;157;0x60000000;0x60000000;AS65089;AS3661;24;24;00000000;syn(2), push(8), ack(16);7770;3
egress;Forwarded;185.233.x.x;78.128.x.x;icmp (1);Echo-reply (0);Echo-reply (0);157;195;0x60000000;0x60000000;AS205002;AS65089;22;24;00000000;;13440;240;56
egress;Forwarded;2a00:1028:x:d86a:x:x:x:x;2001:718:x:1f:x:x:x:x;ipv6-icmp (58);0;128;157;195;0x60000000;0x60000000;AS5610;;32;64;00000000;;117520;1130;104
egress;Forwarded;137.189.x.x;78.128.x.x;tcp (6);60378;https (443);157;195;0x60000000;0x60000000;AS3661;AS65089;24;24;00000000;push(8), ack(16);1980;10;198
egress;Forwarded;185.211.x.x;78.128.x.x;icmp (1);Echo-reply (0);Echo-reply (0);157;195;0x60000000;0x60000000;AS205619;AS65089;22;24;00000000;;10880;160;68
egress;Forwarded;185.108.x.x;78.128.x.x;icmp (1);Echo-reply (0);Echo-reply (0);157;195;0x60000000;0x60000000;AS20609;AS65089;22;24;00000000;;6120;90;68
```

monitoring provozu na bázi toků (flow-based)

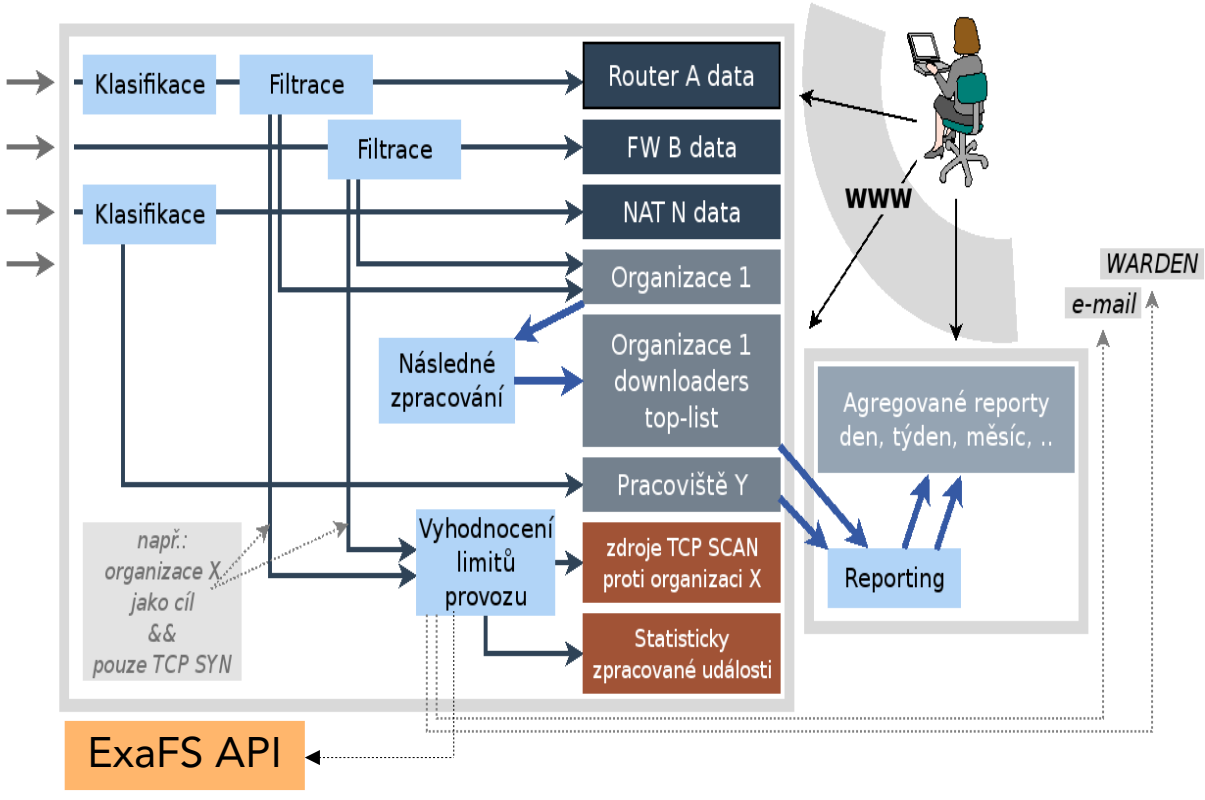
- *exotika ?* → ***standardní součást správy sítě a dohledu !!!***
- schopnost dohledat konkrétní provoz
- schopnost libovolné zpětné analýzy provozu
- schopnost vysledovat trendy, anomálie, …

→ schopnost řídit infrastrukturu a mít ji pod kontrolou

- *..a je jedno jakým nástrojem..*

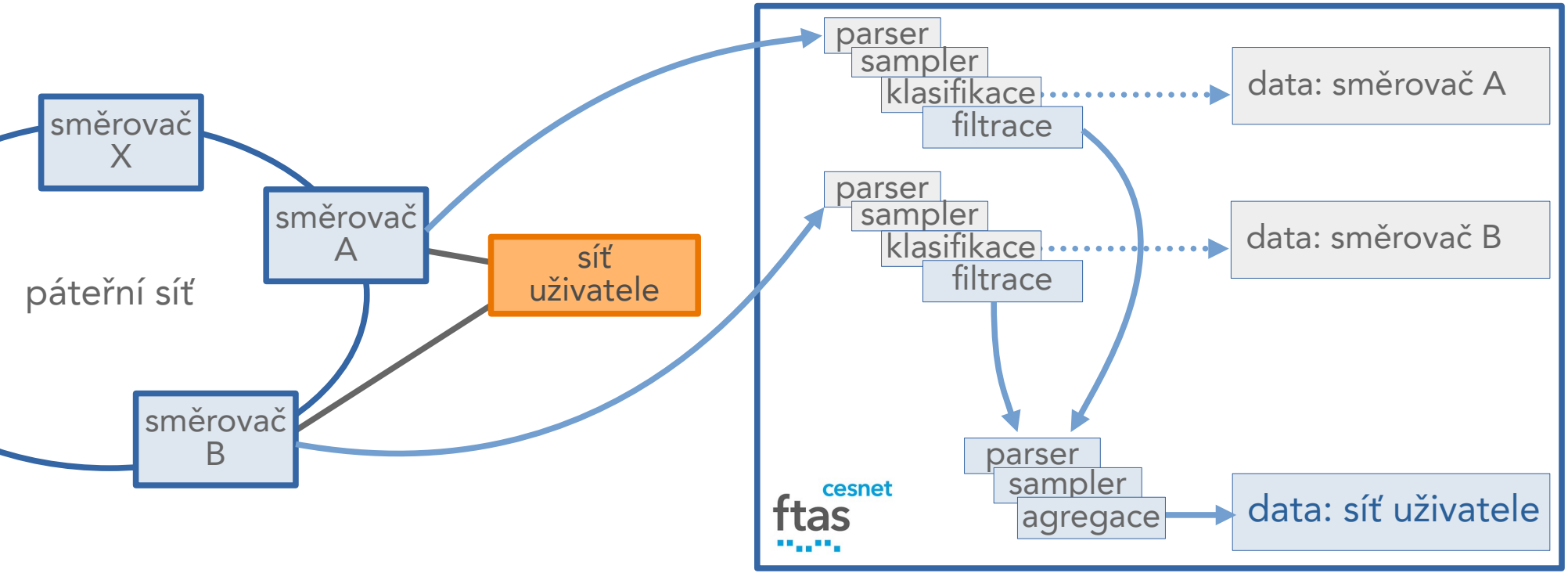
FTAS – nástroj pro sběr, zpracování, uchování a vizualizaci flow-based dat

- vstupy
  - Netflow 1, 5, 7, 9, 10, NSEL, IPFIX, sFlow
- zpracování
  - replikace, klasifikace,filtrace
  - detekce anomálií
    - notifikace, automatická regulace provozu
  - uchování dat
  - ex-post statistiky
- zpřístupnění
  - UI, API, statické výstupy
- kromě faktické správy sítí použití mj.
  - uchování provozních a lokalizačních údajů
  - detekce kybernetických bezpečnostních událostí



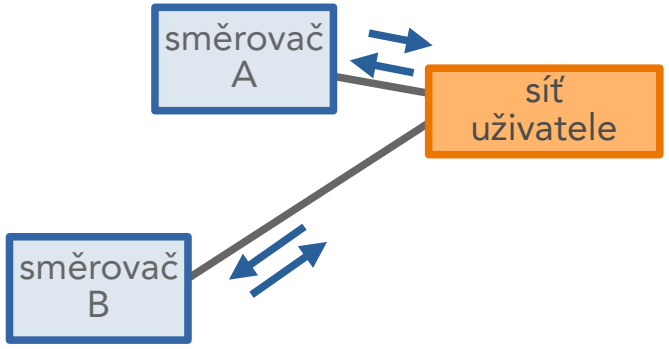
Základní varianta monitoringu (sítě připojené do e-infrastruktury CESNET)

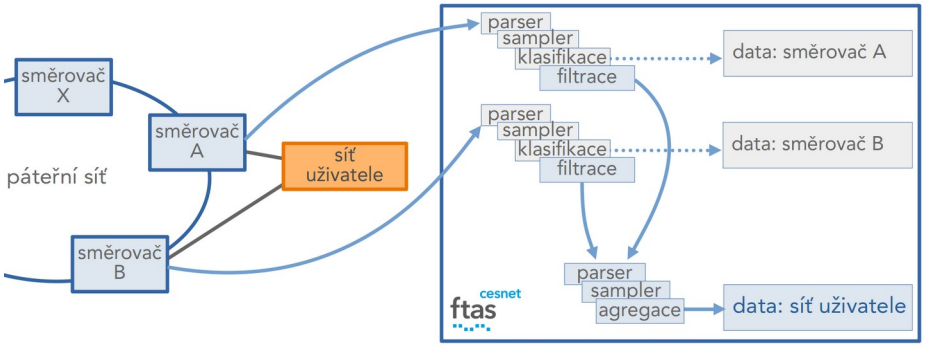
- **data z páteřních prvků**, zpracování v centrální instalaci **FTAS v e-infrastruktuře**



Základní varianta monitoringu (sítě připojené do e-infrastruktury CESNET)

- **data z páteřních prvků**, zpracování v centrální instalaci **FTAS v e-infrastruktuře**
- filtr z dat směrovačů
  - nejbližší koncové síti (primární, záložní připojení)
- z pohledu uživatele „snadné na realizaci“
  - vše v centrální instalaci v e-infrastruktuře
- viditelnost provozu ?
- vzorkování ?
- doba uchování dat ?
- přístup k datům ?





Základní varianta monitoringu (sítě připojené do e-infrastruktury CESNET)

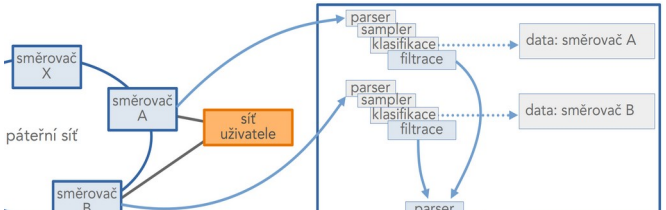
- **data z páteřních prvků**, zpracování v centrální instalaci **FTAS v e-infrastruktuře**
- vypovídací hodnota ?

příklad informací z páteřního L3 prvku

- infomace o doručení
- směr a trasa doručení

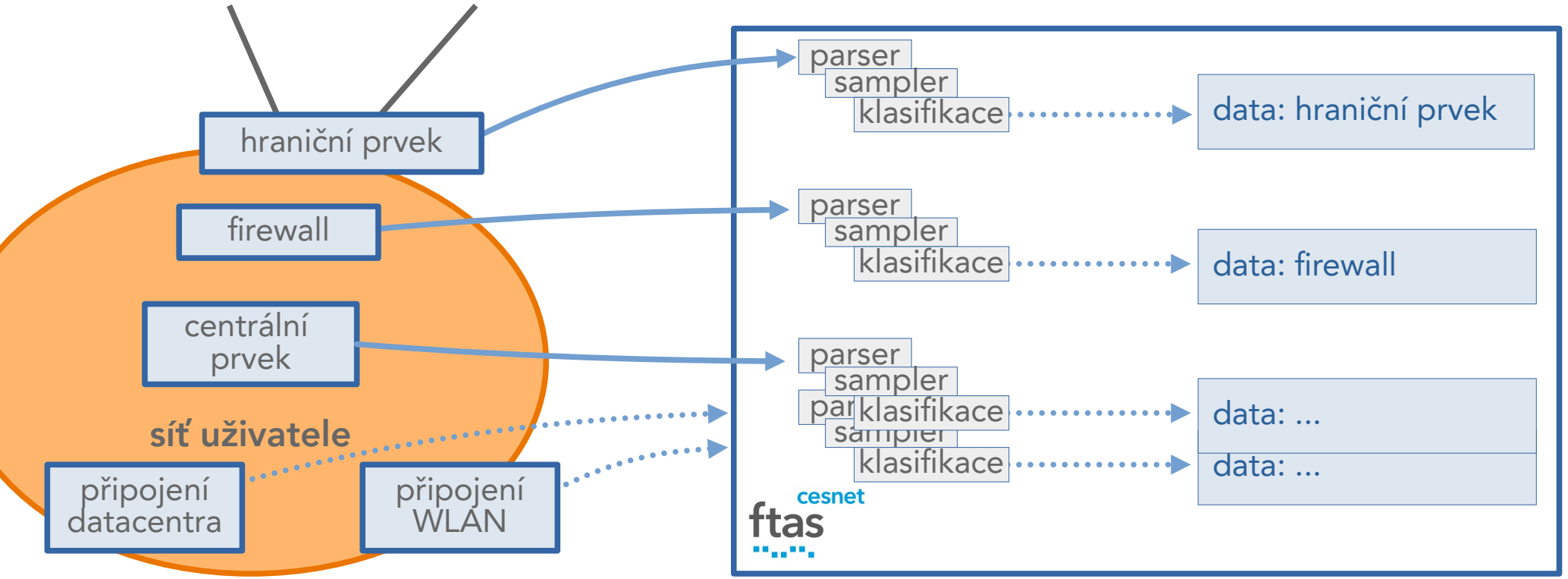
o	>	Flow-Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	TOS-flags	TCP-flags	Flow-Start [CET]
1.		egress	Forwarded	82.142.x.x	158.194.x.x	tcp (6)	https (443)	7076	101	127	00000000	push(8), ack(16)	23/01/31 08:20:32.005
2.		ingress	Forwarded	158.194.x.x	64.250.x.x	udp (17)	echo (7)	echo (7)	127	101	00000000		23/01/31 08:20:32.028
3.		egress	Forwarded	95.165.x.x	158.194.x.x	udp (17)	54717	echo (7)	101	127	10100100		23/01/31 08:20:32.029
4.		egress	Forwarded	49.12.x.x	158.194.x.x	udp (17)	56801	17052	101	127	00000000		23/01/31 08:20:32.057
5.		ingress	Forwarded	158.194.x.x	176.102.x.x	udp (17)	57297	53566	127	101	00000000		23/01/31 08:20:32.082
6.		ingress	Forwarded	158.194.x.x	185.161.x.x	udp (17)	ipsec-nat-t (4500)	ipsec-nat-t (4500)	127	101	00000000		23/01/31 08:20:32.092
7.		egress	Forwarded	13.40.x.x	158.194.x.x	tcp (6)	9000	26379	101	127	00000000	push(8), ack(16)	23/01/31 08:20:32.105
8.		egress	Forwarded	185.17.x.x	158.194.x.x	tcp (6)	https (443)	62341	101	127	00000000	ack(16)	23/01/31 08:20:32.117
9.		ingress	Forwarded	158.194.x.x	38.99.x.x	tcp (6)	62254	https (443)	127	101	00000000	push(8), ack(16)	23/01/31 08:20:32.152
10.		ingress	Forwarded	158.194.x.x	46.227.x.x	tcp (6)	24888	1025	127	101	00000000	push(8), ack(16)	23/01/31 08:20:32.162
o	>	Flow-Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	TOS-flags	TCP-flags	Flow-Start

Flow-End [CET]	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt	Flow-Data-S
23/01/31 08:20:42.379	19.004 KB	224.247 KB	13.000 p	153.000 p	1461.85	1	CESNET3: R
23/01/31 08:21:02.940	703.788 KB	8.436 MB	669.000 p	8.018 Kp	1052	3	CESNET3: R
23/01/31 08:20:42.051	96.000 B	1.132 KB	3.000 p	35.000 p	32	1	CESNET3: R
23/01/31 08:20:53.804	32.913 KB	388.372 KB	77.000 p	908.000 p	427.44	2	CESNET3: R
23/01/31 08:20:54.454	1.396 KB	16.472 KB	22.000 p	258.000 p	63.45	2	CESNET3: R
23/01/31 08:20:54.171	16.256 KB	191.820 KB	28.000 p	330.000 p	580.57	2	CESNET3: R
23/01/31 08:20:42.678	160.000 B	1.888 KB	3.000 p	35.000 p	53.33	1	CESNET3: R



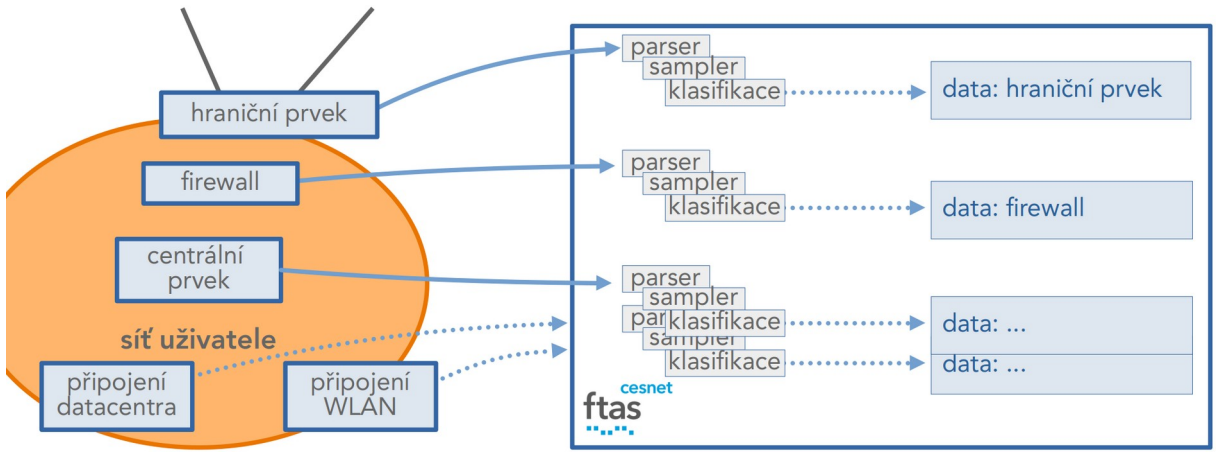
Varianta a) monitoringu z dat vlastní sítě

- export dat **z prvků vlastní sítě**, zpracování v centrální instalaci **FTAS v e-infrastruktuře**



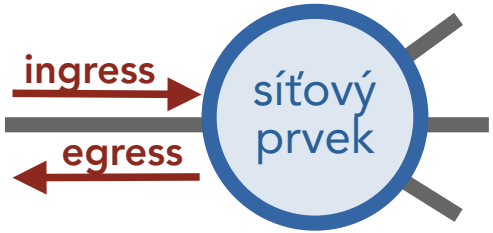
Varianta a) monitoringu z dat vlastní sítě

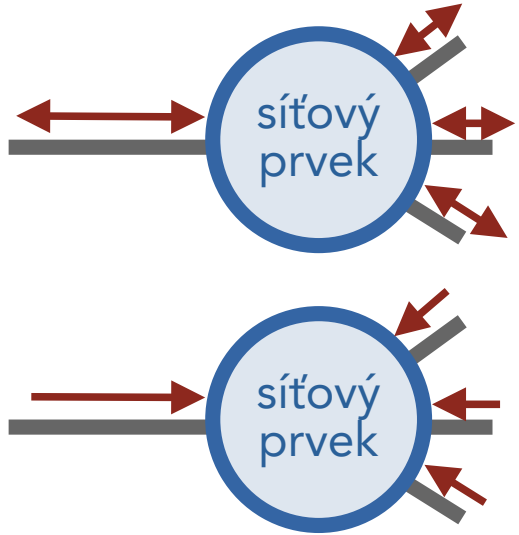
- export dat **z prvků vlastní sítě**, zpracování v centrální instalaci **FTAS v e-infrastruktuře**
- export dat ze síťových prvků
  - egress+ingress na relevantních/všech rozhraních / ..ingress na všech
- snadné na realizaci
  - zpracování, uchování, vizualizace v centrální instalaci v e-infrastruktuře
- nemáte vhodné prvky ?
  - např. ipfixprobe (CESNET)
  - další SW/HW řešení
- viditelnost provozu ?
- vzorkování ?
- doba uchování dat ?
- přístup k datům ?

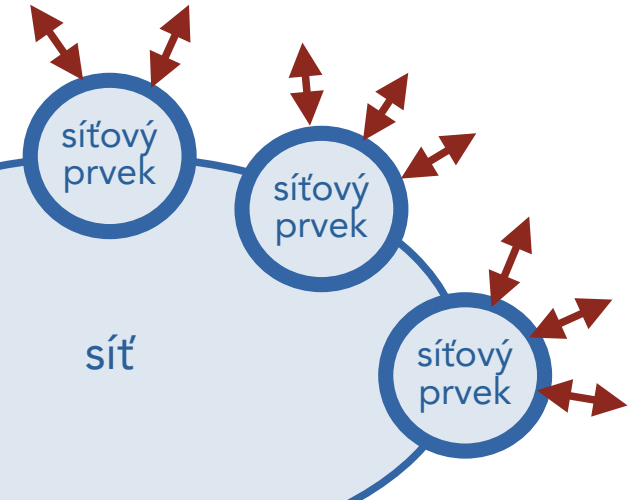


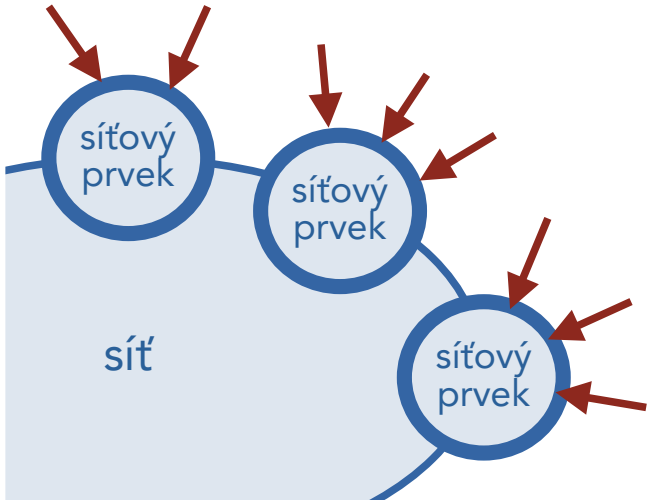
Export dat z prvků vlastní sítě

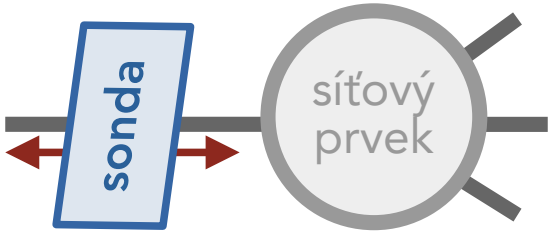
- mechanismus exportu ?
  - ingress vs. egress vs. ingress+egress
- sampling ?
  - zátěž vs. vypovídací hodnota











Export dat z prvků vlastní sítě

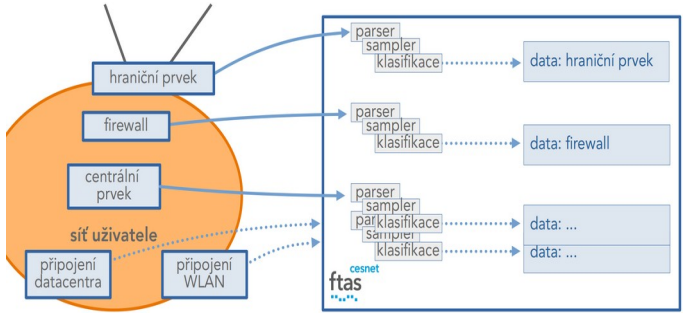
- vypovídací hodnota ?

příklad centrální/hraniční L3 prvek

- infomace o doručení
- směr a trasa doručení

o	>	Flow-Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Src-Bitmask	Dst-Bitmask
1.		egress	Forwarded	85.71.x.x	193.84.x.x	udp (17)	53994	openvpn (1194)	41	82	16	20
2.		egress	Forwarded	184.104.x.x	195.113.x.x	tcp (6)	https (443)	59299	41	25	0	24
3.		egress	Forwarded	184.104.x.x	195.113.x.x	tcp (6)	https (443)	35950	41	25	0	24
4.		egress	Forwarded	142.251.x.x	195.113.x.x	tcp (6)	https (443)	55029	41	287	24	32
5.		egress	Forwarded	52.112.x.x	195.113.x.x	udp (17)	3480	50035	41	287	14	32
6.		ingress	Forwarded	193.84.x.x	52.114.x.x	tcp (6)	50020	https (443)	82	41	20	14
7.		egress	Forwarded	52.112.x.x	195.113.x.x	udp (17)	3480	50036	41	287	14	32
8.		ingress	Forwarded	195.113.x.x	52.114.x.x	udp (17)	50031	3480	287	41	32	14
9.		egress	Forwarded	2.22.x.x	195.113.x.x	tcp (6)	http (80)	34291	41	287	24	24
10.		ingress	Forwarded	195.113.x.x	208.92.x.x	tcp (6)	54825	https (443)	316	41	28	0
o	>	Flow-Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Src-Bitmask	Dst-Bitmask

TOS-flags	TCP-flags	Nexthop	Flow-Start [CET]	Flow-End [CET]	Bytes-measured	Pkts-measured
11000100		195.178.x.x	23/01/31 13:46:13.032	23/01/31 13:46:43.860	159.870 KB	269.000 p
00000000	push(8), ack(16)	195.178.x.x	23/01/31 13:46:13.158	23/01/31 13:46:47.149	23.787 KB	30.000 p
00000000	push(8), ack(16)	195.178.x.x	23/01/31 13:46:13.187	23/01/31 13:46:43.136	34.034 KB	44.000 p
00000000	push(8), ack(16)	0.0.x.x	23/01/31 13:46:13.328	23/01/31 13:46:28.600	1.878 KB	7.000 p
00000000		0.0.x.x	23/01/31 13:46:13.911	23/01/31 13:46:53.154	726.336 KB	1.003 Kp
00000000	push(8), ack(16)	195.113.x.x	23/01/31 13:46:13.924	23/01/31 13:46:53.200	501.886 KB	654.000 p
00000000		0.0.x.x	23/01/31 13:46:13.934	23/01/31 13:46:53.208	669.286 KB	977.000 p
00000000		195.113.x.x	23/01/31 13:46:13.948	23/01/31 13:46:43.529	35.371 KB	92.000 p
10100100	push(8), ack(16)	195.113.x.x	23/01/31 13:46:14.020	23/01/31 13:46:28.073	85.020 KB	57.000 p
00000000	ack(16)	195.113.x.x	23/01/31 13:46:14.026	23/01/31 13:46:43.676	2.392 KB	46.000 p
TOS-flags	TCP-flags	Nexthop	Flow-Start	Flow-End	Bytes-measured	Pkts-measured



Export dat z prvků vlastní sítě

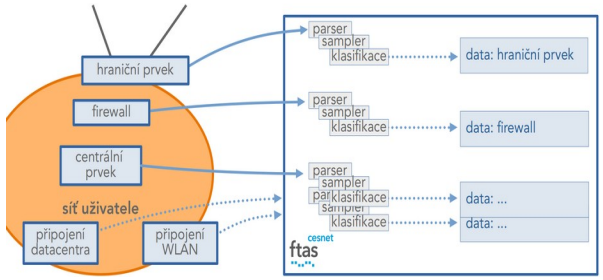
- vypovídací hodnota ?

příklad FW, s překladem adres

- plná překladová informace
- stavová infomace (FW-Event)

o	>	FW-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNAPTPort
1.		Flow update	10.77.x.x	10.77.x.x	10.77.x.x	10.77.x.x	tcp (6)	49733	microsoft-ds (445)	49733	microsoft-ds (445)
2.		Flow update	10.77.x.x	10.77.x.x	10.77.x.x	10.77.x.x	tcp (6)	microsoft-ds (445)	49733	microsoft-ds (445)	49733
3.		Flow update	173.194.x.x	10.77.x.x	173.194.x.x	195.113.x.x	udp (17)	https (443)	54746	https (443)	54746
4.		Flow deleted (2034)	90.182.x.x	10.77.x.x	90.182.x.x	195.113.x.x	tcp (6)	https (443)	53128	https (443)	53128
5.		Flow deleted (2034)	88.221.x.x	10.77.x.x	88.221.x.x	195.113.x.x	tcp (6)	https (443)	53568	https (443)	53568
6.		Flow deleted (2034)	90.182.x.x	10.77.x.x	90.182.x.x	195.113.x.x	tcp (6)	https (443)	53124	https (443)	53124
7.		Flow deleted (2034)	10.77.x.x	52.108.x.x	195.113.x.x	52.108.x.x	tcp (6)	54102	https (443)	54102	https (443)
8.		Flow deleted (2034)	40.101.x.x	10.77.x.x	40.101.x.x	195.113.x.x	tcp (6)	https (443)	50073	https (443)	34423
9.		Flow update	10.77.x.x	10.77.x.x	10.77.x.x	10.77.x.x	tcp (6)	microsoft-ds (445)	61735	microsoft-ds (445)	61735
10.		Flow deleted (2039)	150.171.x.x	10.77.x.x	150.171.x.x	195.113.x.x	tcp (6)	https (443)	52806	https (443)	52806
o	>	FW-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNAPTPort

Src-ifIndex	Dst-ifIndex	Flow-Start	Flow-End	Bytes-measured	Pkts-measured	Avr-Pkt-Length	Flow-Cnt
36							
32							
19							
19	35	23/01/31 13:20:43.639	23/01/31 13:20:52.519	15.848 MB	12.230 Kp	1295.83	2
19	35	23/01/31 13:19:49.537	23/01/31 13:20:44.839	15.347 MB	13.642 Kp	1125.00	2
19	35	23/01/31 13:20:33.559	23/01/31 13:20:42.499	14.864 MB	11.472 Kp	1295.66	2
35	19	23/01/31 13:06:04.931	23/01/31 13:21:01.260	14.640 MB	11.138 Kp	1314.38	2
19	35	23/01/31 09:25:54.886	23/01/31 13:20:44.839	13.690 MB	13.866 Kp	987.32	2
32	35	23/01/31 13:19:52.577	23/01/31 13:20:53.769	10.541 MB	12.891 Kp	817.67	1
19	36	23/01/31 13:18:16.434	23/01/31 13:20:50.839	10.139 MB	7.981 Kp	1270.33	2



Export dat z prvků vlastní sítě

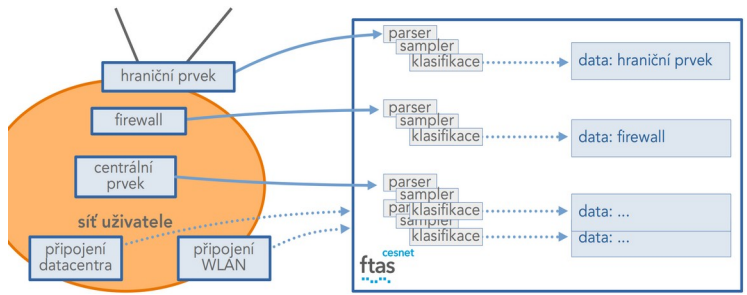
- vypovídací hodnota ?

příklad ipfixprobe sondy

- + L2, + TLS-SNI
- - informace o doručení (stav a kudy) ..u sond z principu nelze

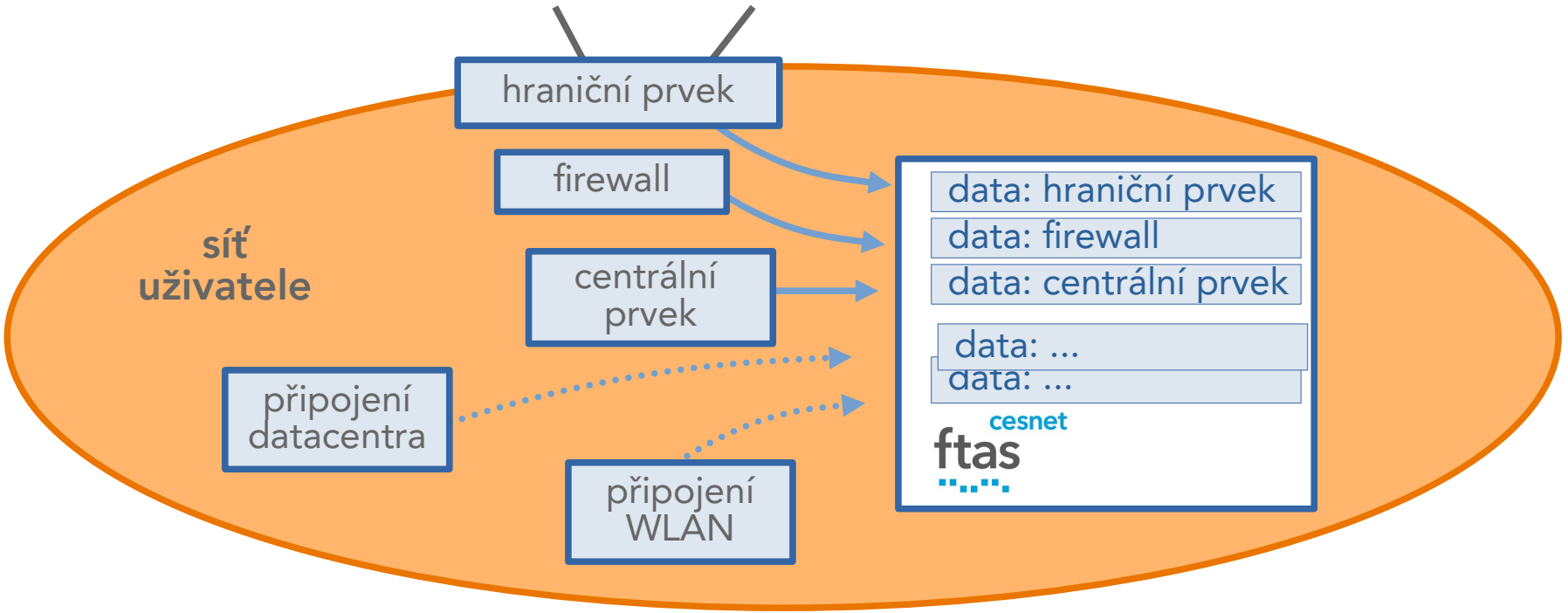
o >	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-MAC-Addr	Dst-MAC-Addr	TCP-flags
1.	195.113.x.x	74.125.x.x	tcp (6)	63770	https (443)	00:09:0f:09:0	00:00:5e:00	fin(1), syn(2), push(8), ack(16)
2.	2001:718:x:105:x:x:x:x	2620:100:x:22:x:x:x:x	tcp (6)	50055	https (443)	00:09:0f:09:0	00:00:5e:00	push(8), ack(16)
3.	78.128.x.x	52.239.x.x	tcp (6)	57806	https (443)	00:09:0f:09:0	00:00:5e:00	syn(2), push(8), ack(16)
4.	195.113.x.x	52.108.x.x	tcp (6)	50949	https (443)	00:09:0f:09:0	00:00:5e:00	syn(2), push(8), ack(16)
5.	2607:f8b0:x:20:x:x:x:x	2001:718:x:601:x:x:x:x	tcp (6)	44639	smtp (25)	00:09:0f:09:0	00:50:56:b6	fin(1), syn(2), push(8), ack(16)
6.	2001:718:x:105:x:x:x:x	2620:100:x:22:x:x:x:x	tcp (6)	49917	https (443)	00:09:0f:09:0	00:00:5e:00	push(8), ack(16)
7.	195.113.x.x	142.251.x.x	tcp (6)	63362	https (443)	00:09:0f:09:0	00:00:5e:00	fin(1), syn(2), push(8), ack(16)
						00:50:56:89:8	00:09:0f:09:	syn(2), push(8), ack(16)
						00:09:0f:09:0	00:00:5e:00	syn(2), push(8), ack(16)

TLS-SNI	Bytes-estimated	Pkts-estimated	Flow-Cnt
gcs-eu-00002.content-storage-upload.googleapis.com	6.814 MB	3.016 Kp	1
edge.dropboxstatic.com	6.351 MB	78.780 Kp	1
onedriveclubprodbn20049.blob.core.windows.net	3.238 MB	967.000 p	1
euc-powerpoint.officeapps.live.com	2.862 MB	15.646 Kp	1
	2.848 MB	1.507 Kp	1
edge.dropboxstatic.com	2.599 MB	39.393 Kp	1
gcs-eu-00002.content-storage-upload.googleapis.com	2.373 MB	815.000 p	1
.osu.cz	1.718 MB	227.000 p	1
rupload.facebook.com	1.403 MB	644.000 p	1



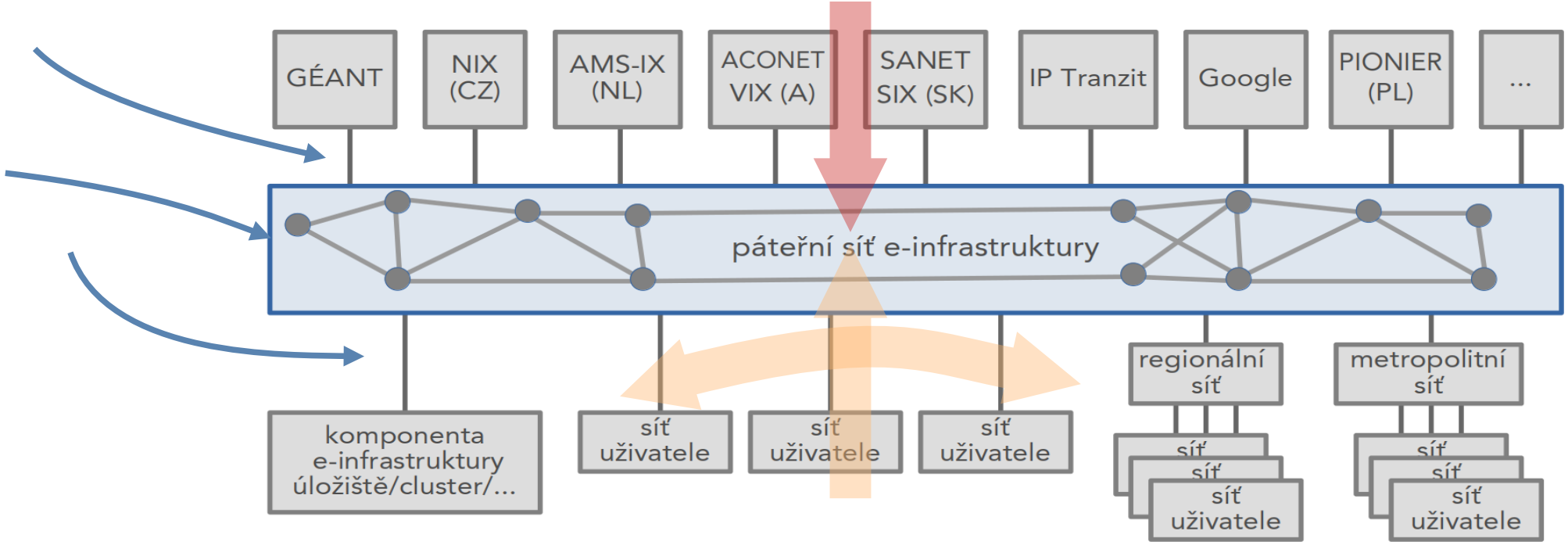
Varianta b) monitoringu z dat vlastní sítě - nezávislá

- export dat **z prvků vlastní sítě**, zpracování ve **vlastní instanci FTAS**
- technicky analogické, informačně identické s předchozím případem
- lokální instalace → dostupnost bez ohledu na stav vlastní konektivity *vs. zašifrovali nám to ;-(*



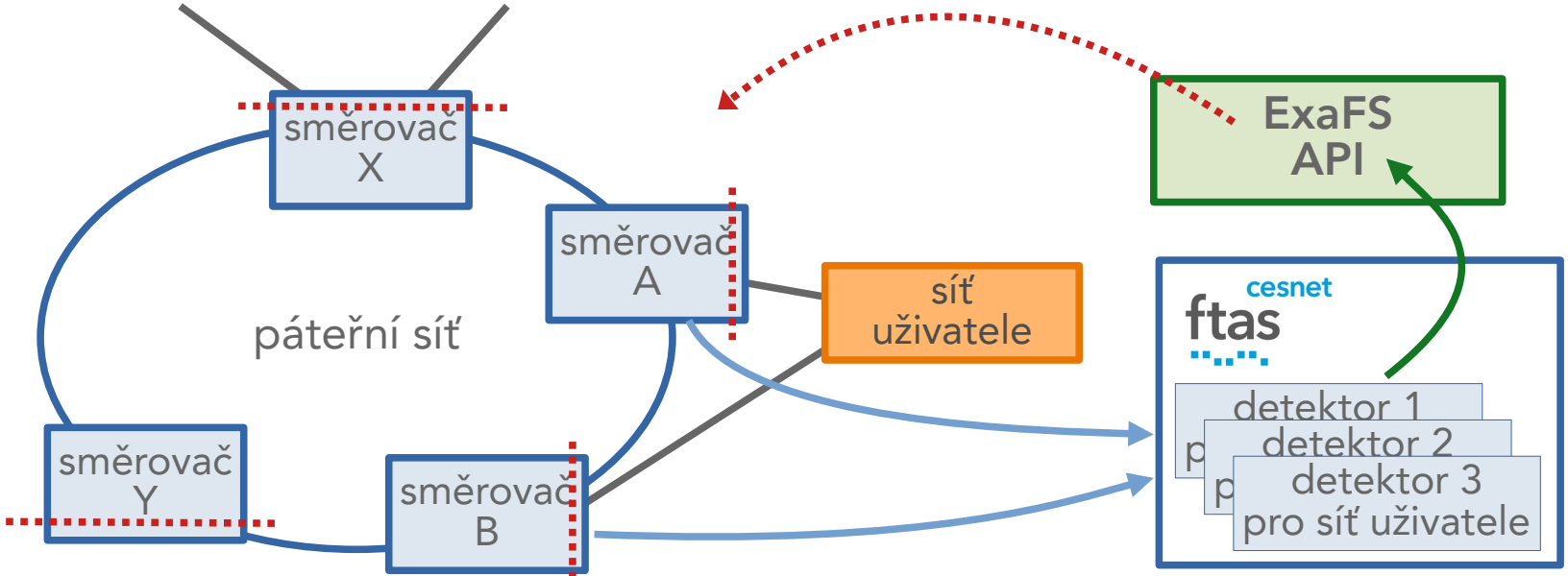
Detekce a automatická obrana proti typickým síťovým útokům a anomáliím

- **pro celý AS**
  - *„konzumují" všichni uživatelé e-infrastruktury (možný whitelisting, specifické limity)*
  - kompromisní nastavení citlivosti detektorů, ochrana infrastruktury, ochrana uživatelů



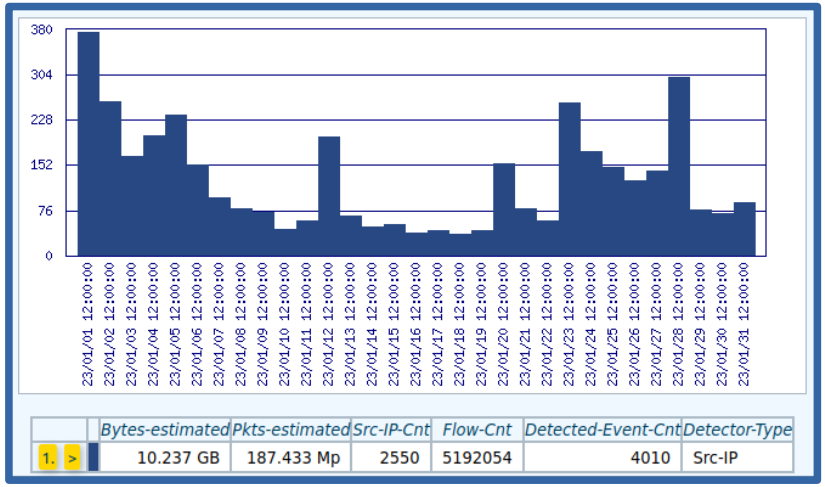
Detekce a automatická obrana proti typickým síťovým útokům a anomáliím

- možné **individuálně pro konkrétního uživatele/skupinu**
- **typické útoky/anomálie** → citlivost detektorů podle požadavků
- **specifické útoky/obtěžování/zájmový provoz** (např. potenciální těžba) → konkrétní charakteristiky/profily provozu
- ve všech variantách nasazení FTAS



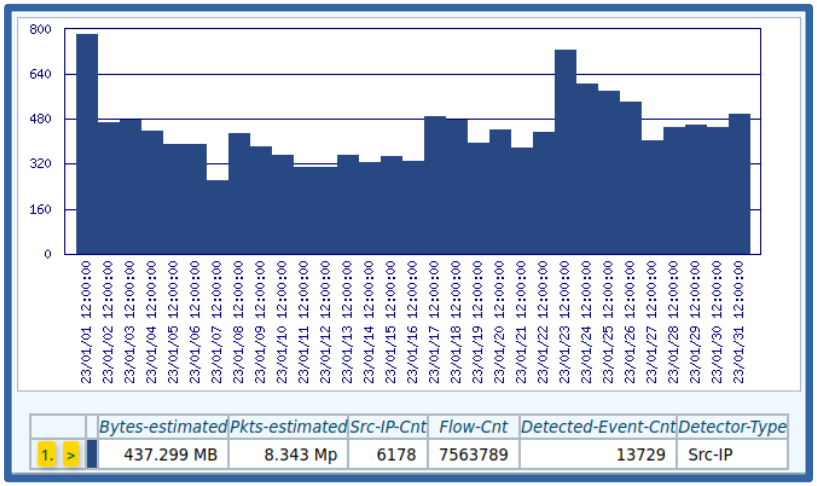
Detekce a automatická obrana konkrétního uživatele/skupiny

- proč i individuálně ?
- dává to smysl ?

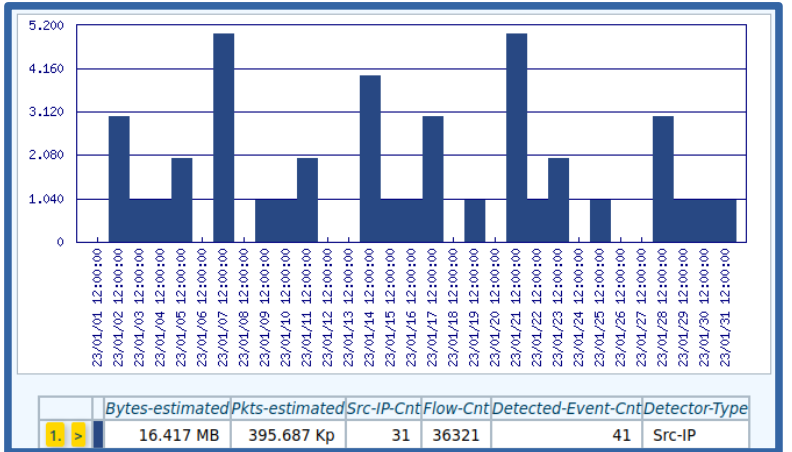


	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Detected-Event-Cnt	Detector-Type
1. >	10.237 GB	187.433 Mp	2550	5192054	4010	Src-IP

vs.



	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Detected-Event-Cnt	Detector-Type
1. >	437.299 MB	8.343 Mp	6178	7563789	13729	Src-IP



	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Detected-Event-Cnt	Detector-Type
1. >	16.417 MB	395.687 Kp	31	36321	41	Src-IP

pozn.: stejný typ detektoru, různí uživatelé (skupiny), různá citlivost

Závěry

- **monitorujme → nebuďme slepí !!!**
  - infrastruktura sítě, její stav, využití, **jaký provoz přenáší**
  - **důležité je vědět, co se v síti děje a v jakém je stavu**
  - ...je jedno jakými nástroji
  - klíčový je personál, který umí informace vyhodnotit a reagovat

- **chcete-li využít FTAS**
  - varianta ?
  - technické řešení ?
  - co a odkud exportovat ?
  - konzultace

sluzby@cesnet.cz


cesnet
Díky za pozornost.