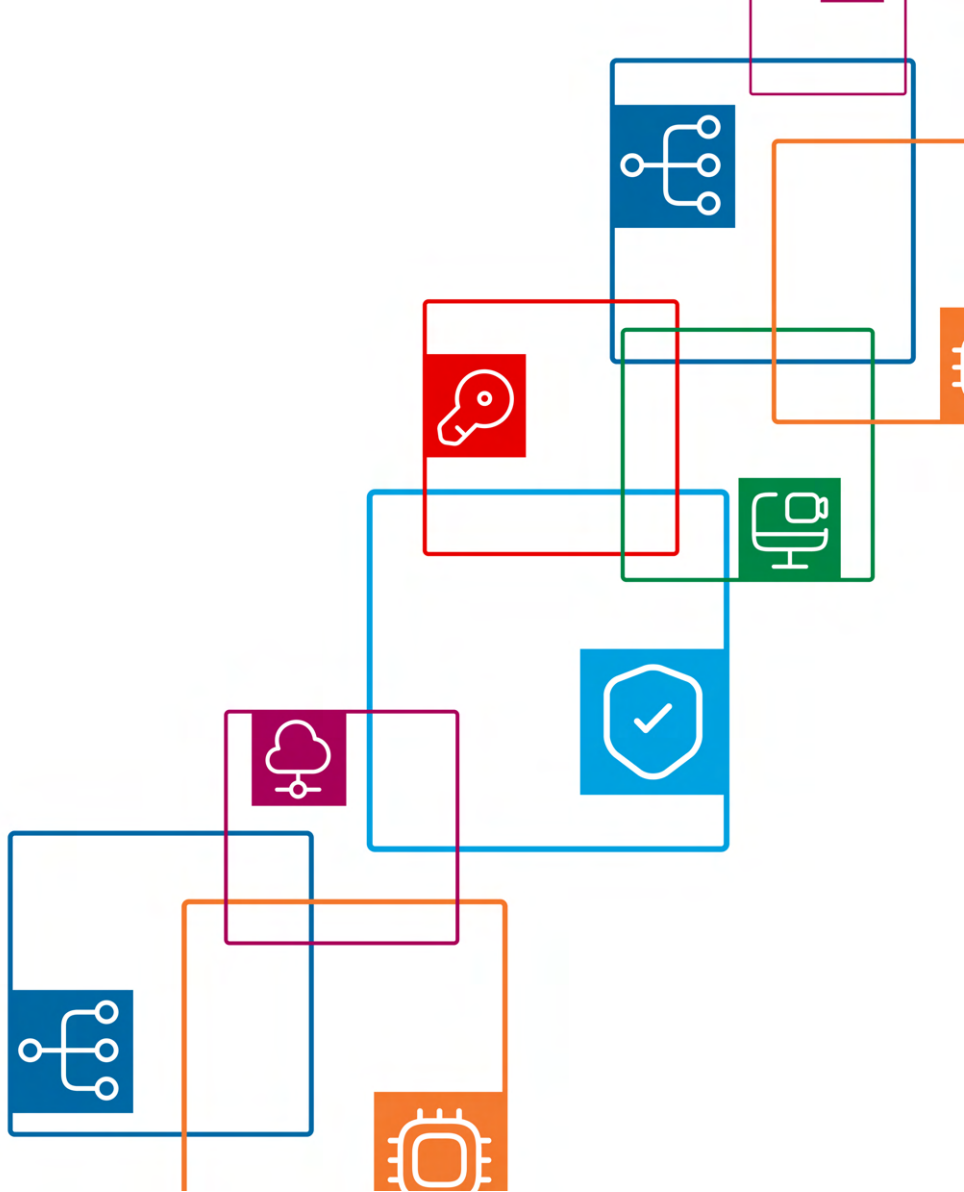
cesnet

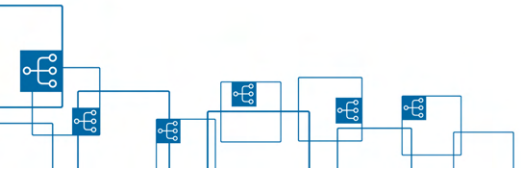
Evoluce obrany sítě CESNET

Tomáš Košňar a
Petr Adamec

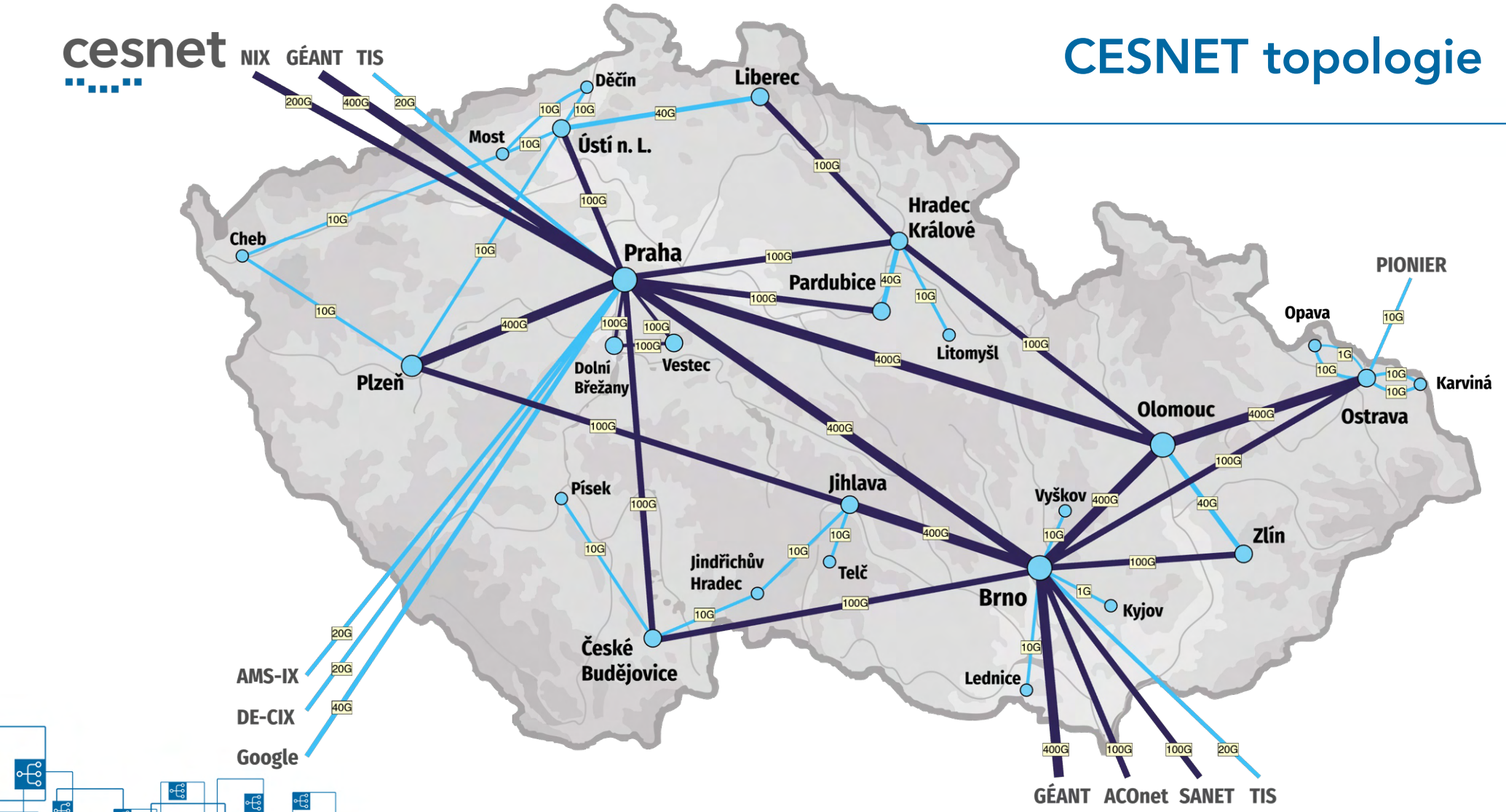
leden 2026
CSNOG Zlín



- Zájmové sdružení právnických osob
  - 1996 – vysoké školy + Akademie věd
  - e-infrastruktura – Velká Infrastruktura pro Výzkum a Vývoj → transport, zpracování, ukládání dat, prostředí pro spolupráci, AAI, ...
  - v oblasti transportu/síťování připojujeme pouze koncové sítě, nikoliv individuální koncové uživatele
    - velké rozdíly ve velikosti sítí (/16 IPv4 vs. malá laboratoř v krajině) a v přenášených objemech
    - většinově nedeterministický charakter provozu



CESNET topologie



cesnet

Evoluce ochrany sítě/uživatelů a síťových prvků

ACL → uRPF → QoS → CoPP

2004 — 2005

Arbor Peakflow SP → RTBH → IPv6 CoPP → Cisco SCE

2007 – 2010
Bez sond, v NetFlow nebyly TCP flagy ☹

2008
CLI

2010

2010
UpStream

cesnet

Evoluce ochrany sítě/uživatelů a síťových prvků v datech

FlowSpec

2016 (2019)
první experimenty

ExaFS

2017 (2019)
CSNOG 2019 J. Verich

RPKI

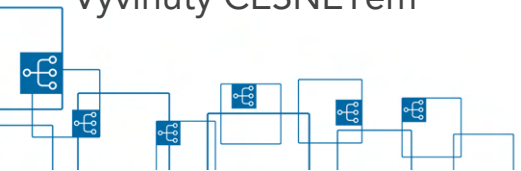
2019
včetně validace
Routinator, RIPE NCC
RPKI Validator

External Scrubbing

2020/2021
Po vyhrůžce a ukázce DDoSu ☹

DDoS Protector

2024 – 2026
Vyvinutý CESNETem



ASPA

2026/2027

BGPsec

Sledujeme vývoj

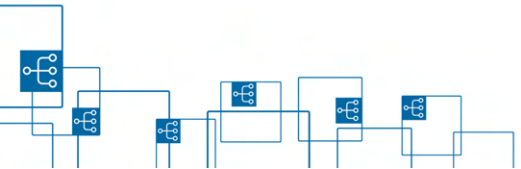
BGP
Route Leak Prevention and Detection Using Roles

Čekáme na implementaci
Route Leak Prevention and Detection Using Roles RFC9234 (CSNOG 2023 A. Zubkov)

- **ExaFS jako prostředek k sjednocení informací**
  - informace o omezeních byla na více místech
  - bylo těžké rychle najít aktuální stav
    - s důrazem na hierarchický přístup k informacím
    - jednoduchým přehledem o všech omezeních

    …a tak se stalo, že ze síťařů byli najednou „bezpečáci“

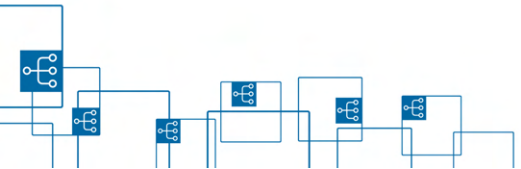
  - posléze jsme přístup poskytli SOCu a správcům připojených organizací (tam, kde to dávalo/dává smysl)

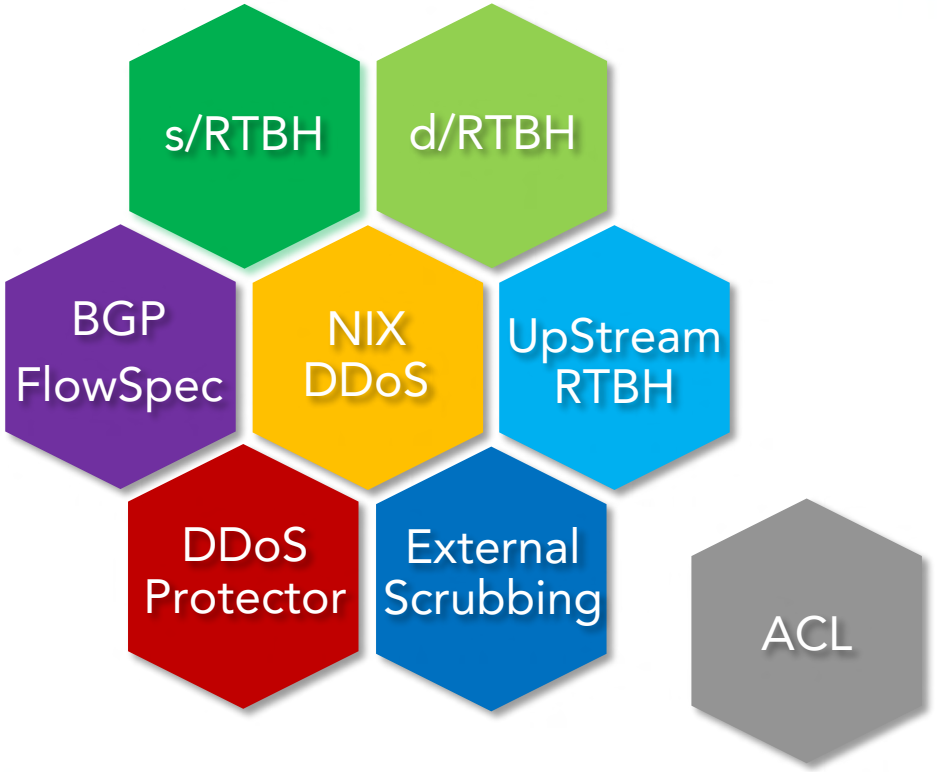


cesnet

ExaFS – začátek automatizace

- **Ruční zadávání pravidel pro omezení provozu**
  - přešli jsme z **ručních** konfigurací přímo ma routerech ke stále ještě **ručnímu** omezení pomocí ExaFS
    - došlo to až k tomu, že bylo nutno zadat více než 100 pravidel za hodinu
  - zprovoznili jsme API a začali plně využívat automatizace



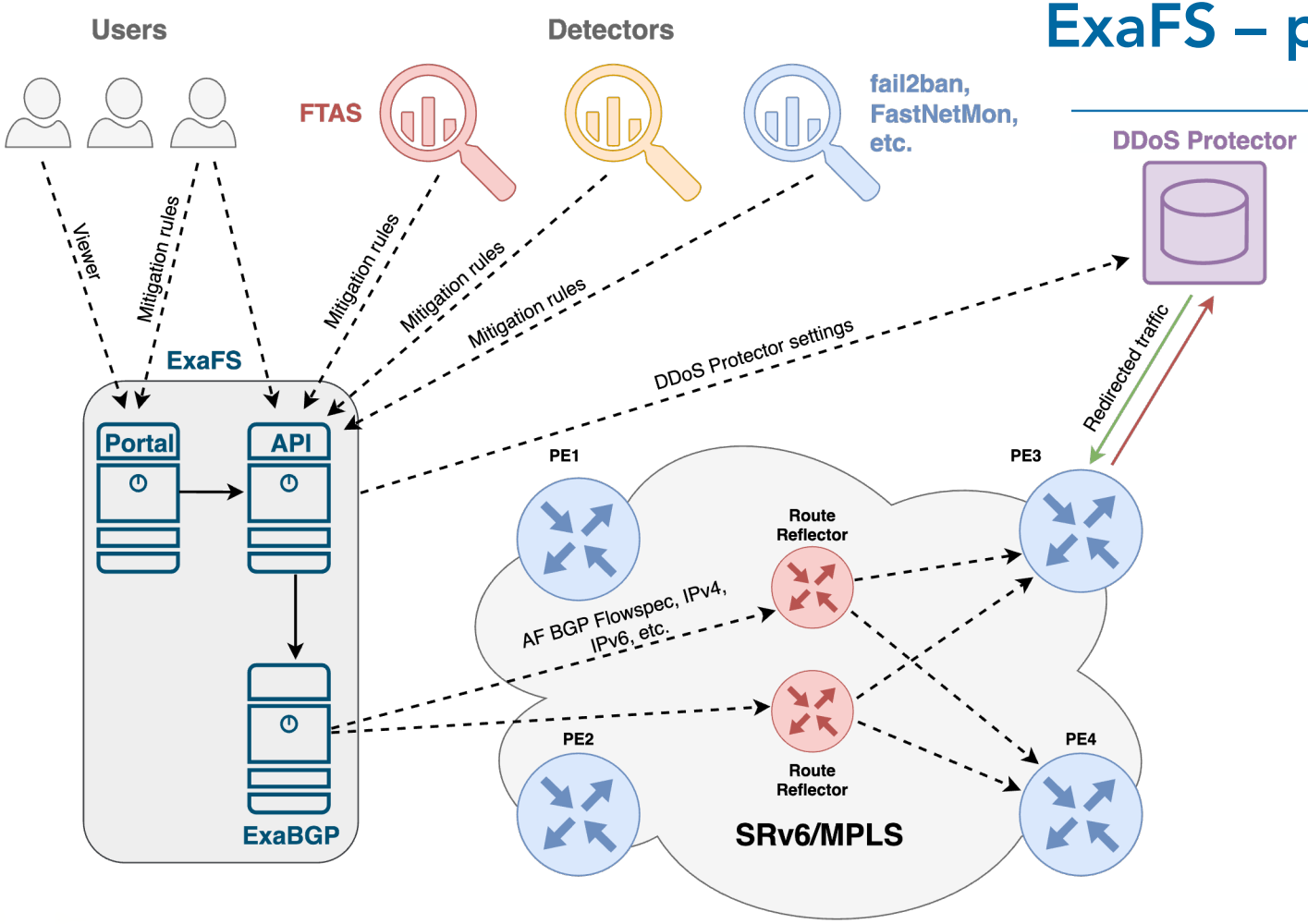


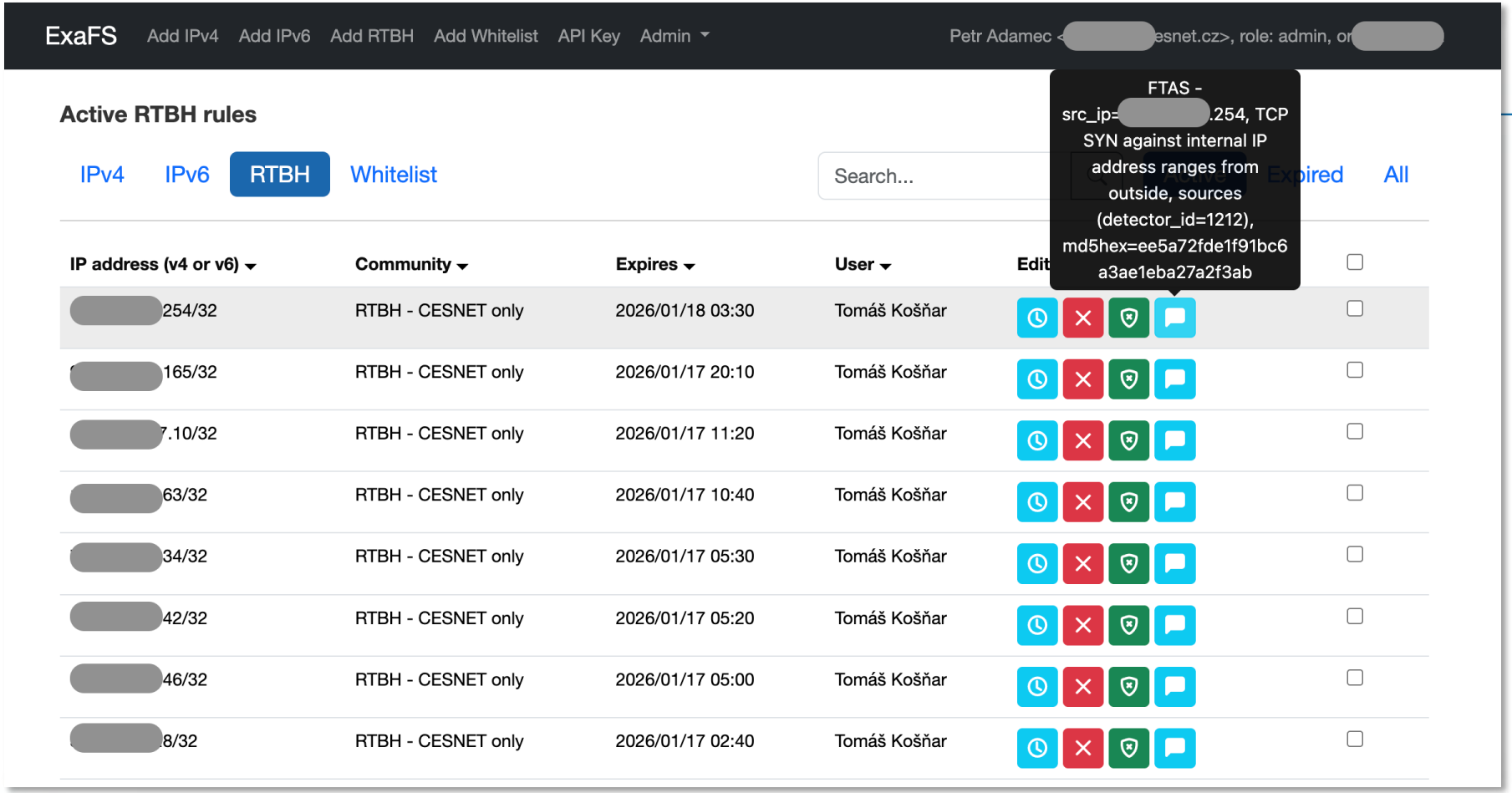
- **Používáme**
  - BGP Community
    - včetně large a extended
  - BGP Address Family
    - IPv4, IPv6, VPNv4, VPNv6
    - Flowspec
      IPv4, IPv6, VPNv4, VPNv6

- **Co bychom rádi – ACL**
  - zatím neimplementováno
  - nikoliv jako zdroj pro běžné ACL

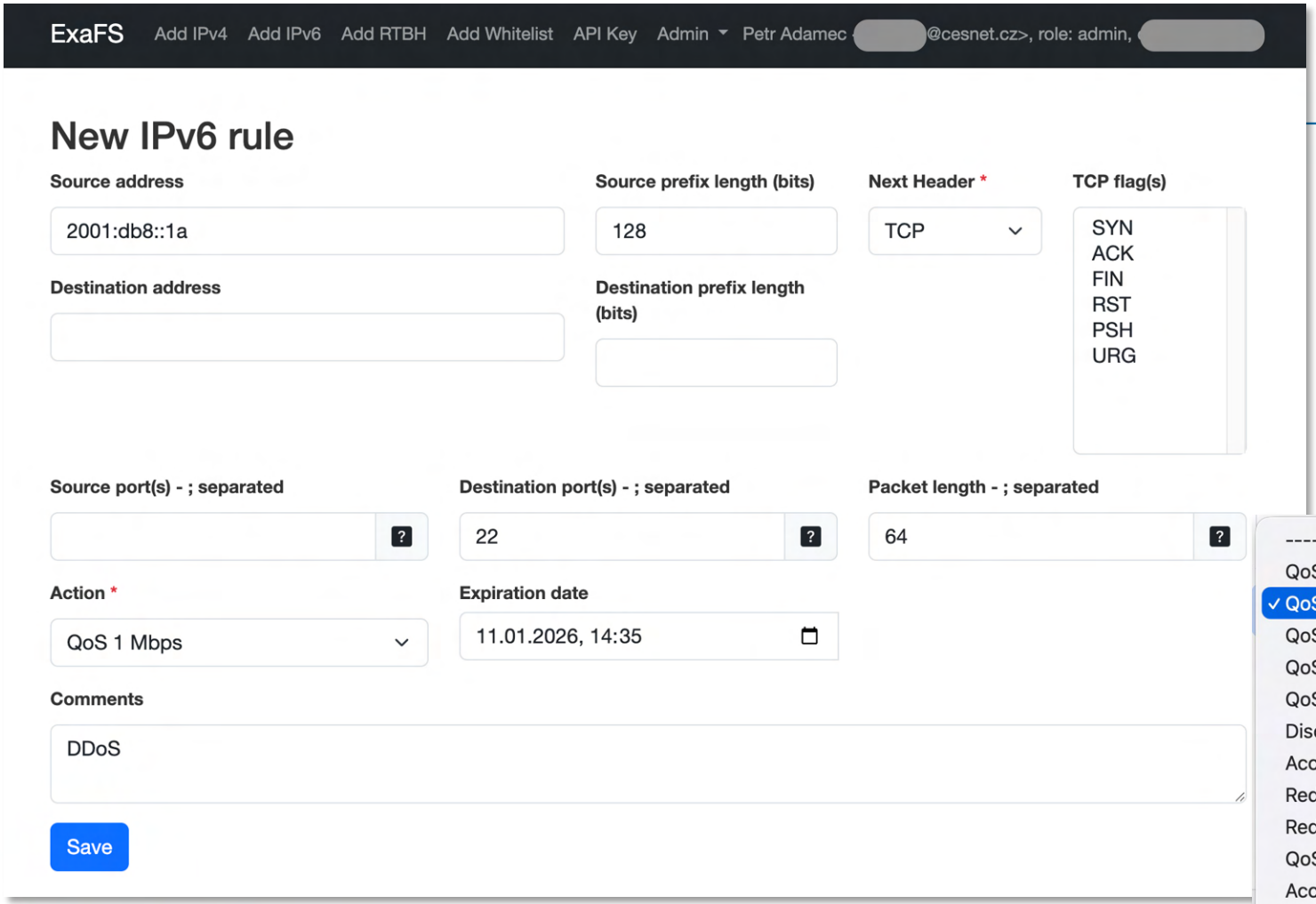
https://github.com/CESNET/exafs

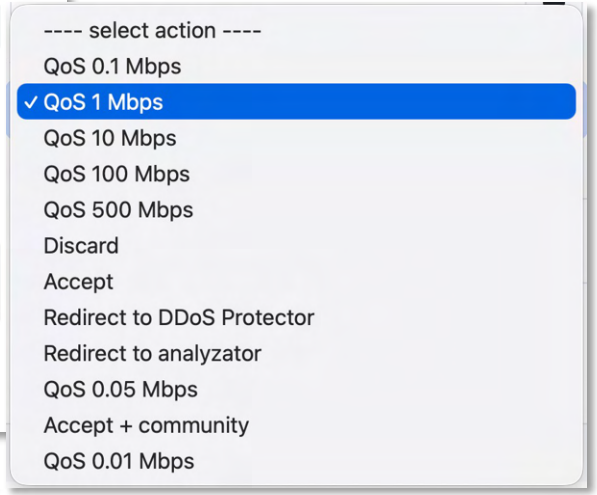
ExaFS – principy




ExaFS
Add IPv4
Add IPv6
Add RTBH
Add Whitelist
API Key
Admin
Petr Adamec
role: admin, or
Active RTBH rules
IPv4
IPv6
RTBH
Whitelist
Search...
Expired
All
IP address (v4 or v6)
Community
Expires
User
Edit
FTAS - src_ip= .254, TCP SYN against internal IP address ranges from outside, sources (detector_id=1212), md5hex=ee5a72fde1f91bc6a3ae1eba27a2f3ab
254/32 RTBH - CESNET only 2026/01/18 03:30 Tomáš Košňar
165/32 RTBH - CESNET only 2026/01/17 20:10 Tomáš Košňar
.10/32 RTBH - CESNET only 2026/01/17 11:20 Tomáš Košňar
63/32 RTBH - CESNET only 2026/01/17 10:40 Tomáš Košňar
34/32 RTBH - CESNET only 2026/01/17 05:30 Tomáš Košňar
42/32 RTBH - CESNET only 2026/01/17 05:20 Tomáš Košňar
46/32 RTBH - CESNET only 2026/01/17 05:00 Tomáš Košňar
8/32 RTBH - CESNET only 2026/01/17 02:40 Tomáš Košňar

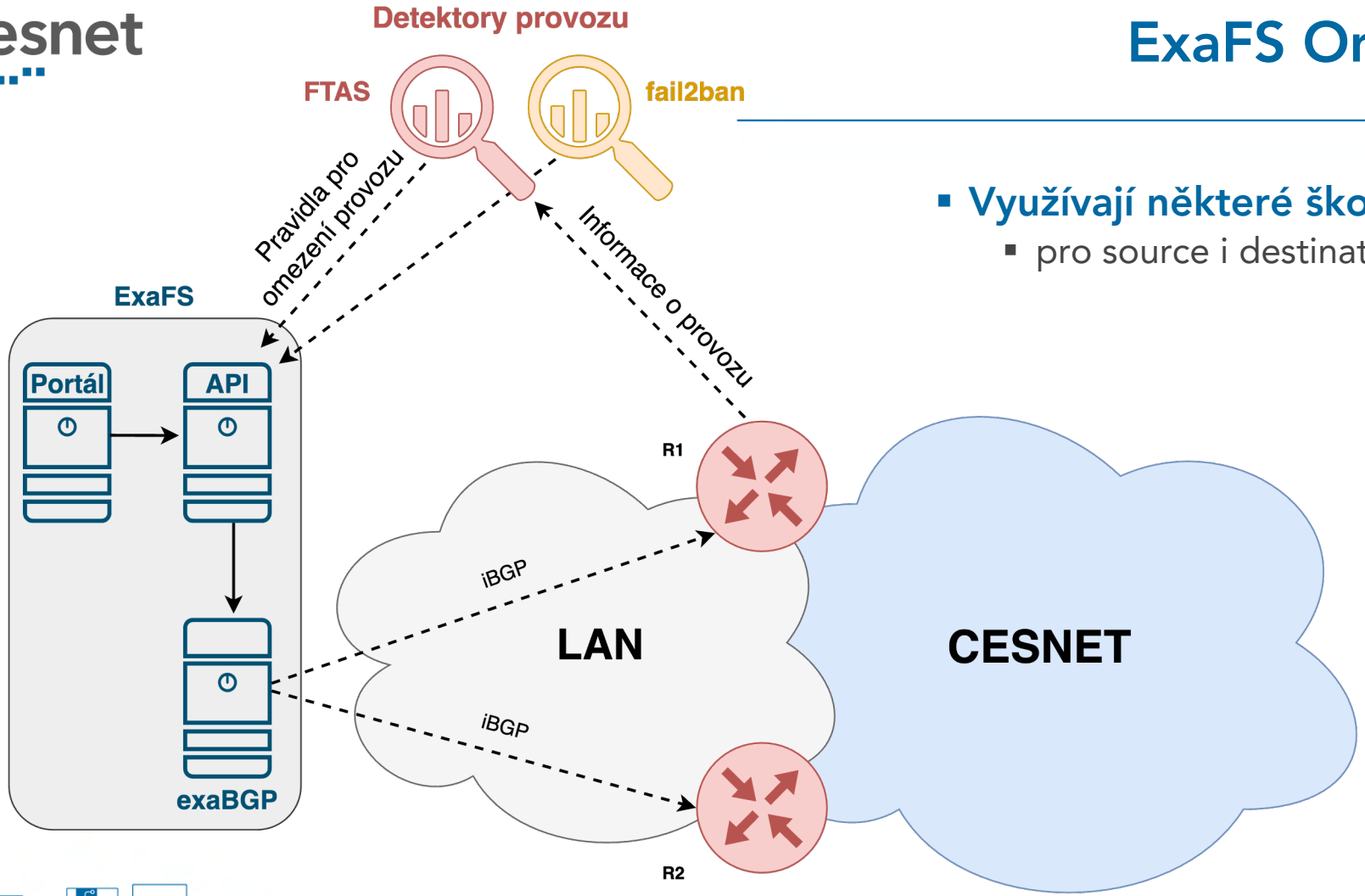
ExaFS


ExaFS
Add IPv4
Add IPv6
Add RTBH
Add Whitelist
API Key
Admin
Petr Adamec
@cesnet.cz>, role: admin,
New IPv6 rule
Source address
2001:db8::1a
Source prefix length (bits)
128
Next Header *
TCP
TCP flag(s)
SYN
ACK
FIN
RST
PSH
URG
Destination address
Destination prefix length (bits)
Source port(s) - ; separated
Destination port(s) - ; separated
22
Packet length - ; separated
64
Action *
QoS 1 Mbps
Expiration date
11.01.2026, 14:35
Comments
DDoS
Save


---- select action ----
QoS 0.1 Mbps
✓ QoS 1 Mbps
QoS 10 Mbps
QoS 100 Mbps
QoS 500 Mbps
Discard
Accept
Redirect to DDoS Protector
Redirect to analyzator
QoS 0.05 Mbps
Accept + community
QoS 0.01 Mbps

ExaFS On-Premise

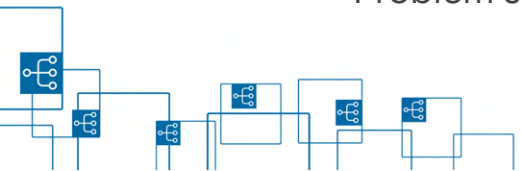
- Využívají některé školy
  - pro source i destination RTBH



cesnet

Cesta slepých uliček 1/2

- **Problémy jednotlivých síťových prvků**
  - momentální problém s ACL (pokud je zároveň aplikován ingress i egress filter)
    - ACL propustí adresy z prefixu 0.0.0.0/8 v síti
    - ACL propustí privátní adresy do NIXu/FENIXu
- **BGP FlowSpec**
  - skutečný limit pravidel na zařízení (IPv4/IPv6)
  - limity pro počet identifikátorů v závislosti na zařízení (momentálně 5 identifikátorů)
  - je implementováno ”rate = 0” jako stavový mechanismus (co musí být při rate>0) nebo jako analogie ACL?
- **Netflow**
  - nastavení NetFlow u jednotlivých platforem
  - nepřesnosti/chyby v exportovaných datech v závislosti na zařízení
    - Problém s TCP flagy (SYN)

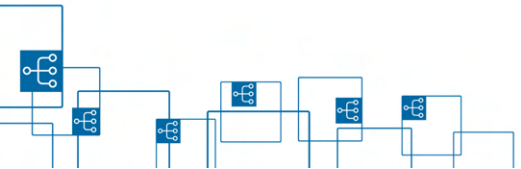


cesnet

Cesta slepých uliček 2/2

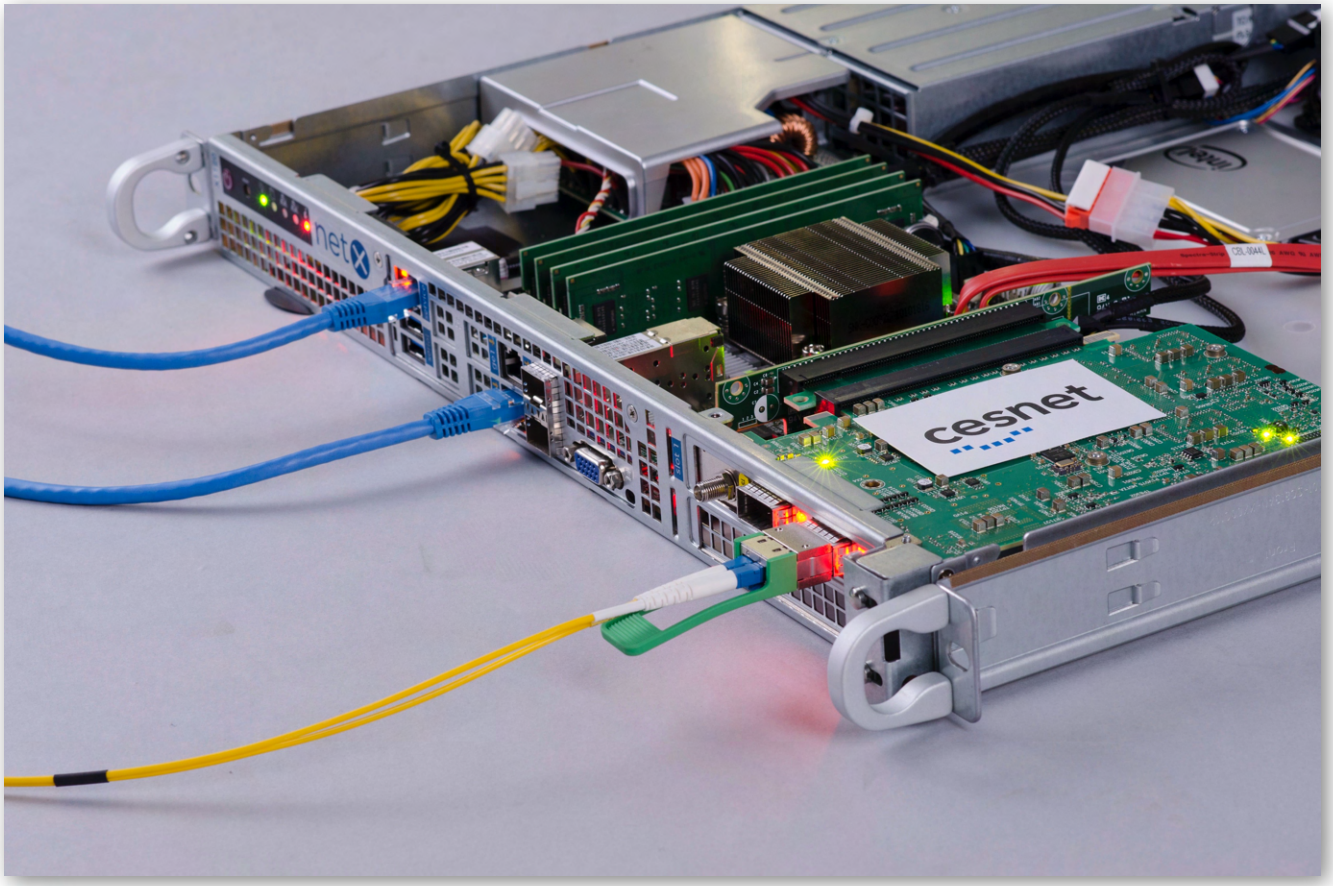
- **ExaFS**
  - při zpřístupnění FlowSpecu uživatel poslal 1700 pravidel s TTL na půl roku (přičemž validita adres z těch událostí byla zhruba na méně než týden)
    - naimplementovali jsme limity pro jednotlivé regulační mechanismy per organizaci

- **False positives**
  - ano, bohužel máme
  - většinou způsobené nestandardním chováním obslužného místa nebo transportu mimo CESNET
  - komplikovaná náprava, proto vznikl v ExaFS **whitelisting**



cesnet

DDoS Protector

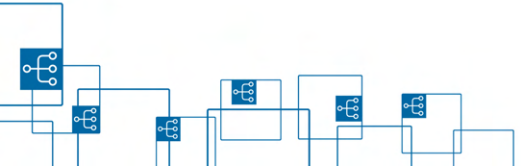


cesnet

DDoS Protector pro zvídavé

- **DDoS Protector**
  - není potřeba FPGA karta – běží na komoditním HW – na síťových kartách od NVIDIA
  - cílová propustnost cca 100Mpps na 16 fyzických CPU jádrech
  - metody zaměřené na ochranu před amplifikačními útoky – SYN floody (včetně Carpet Bombing), ochrana DNS, atd…
  - výzkum metod založených na strojovém učení

Detaily se dozvíte na stánku CESNETu



Automatizovaná obrana sítě

Cíle, strategie

První plán

- **udržet funkčnost a zabránit saturaci**
  - páteřní síť
  - externí propojení
  - přípojky uživatelů

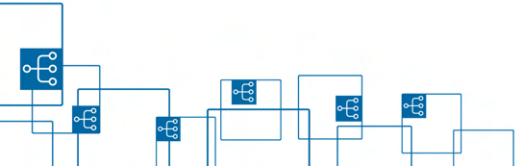
  + funkčnost dalších infrastrukturních prvků

Druhý plán

- **odlehčení uživatelům**
  - infrastruktura, hraniční prvky, obranné prvky, platformy, *obslužné prvky, aplikace*

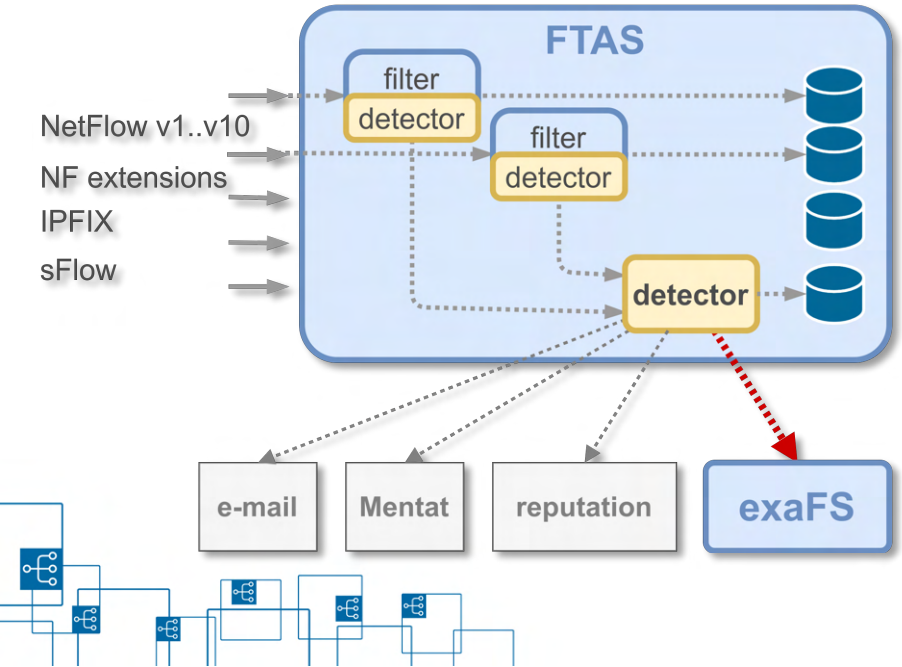
Ošetření / zásahy do provozu

- **provoz z hlediska transportu**
  - anomální, nelegitimní
  - legitimní/standardní
- **původ událostí**
  - „vně“
  - „uvnitř“
- spolupráce s uživateli



Flow-based monitoring – výchozí řízení obrany

- dlouhodobé zkušenosti (začátky v minulém století), vlastní vývoj, vlastní nástroje
- data ze síťových prvků i vlastní sondy

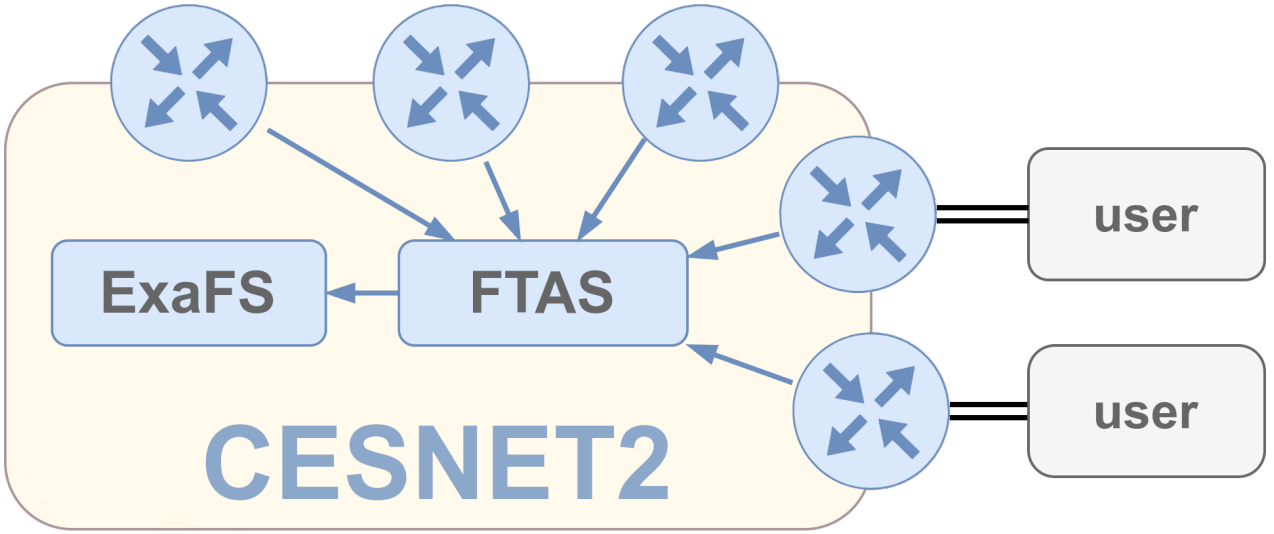


FTAS - zpracování a zpřístupnění flow-based dat

- funkce pro konfiguraci detektorů
- notifikace → analýza, ruční regulace
- zlepšuje se detekce → nelze zvládat ručně
- **automatizace = nutnost**
- **přímé řízení ExaFS API**

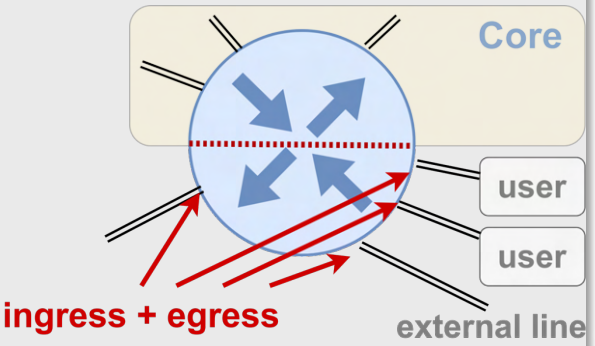
Evoluce architektury

- výchozí model
- je to dobré, funkční, ale..



NetFlow setup

- co? jak? kudy?
- …a hlavně rychle…
- nízký sampling
- nízké timeouty

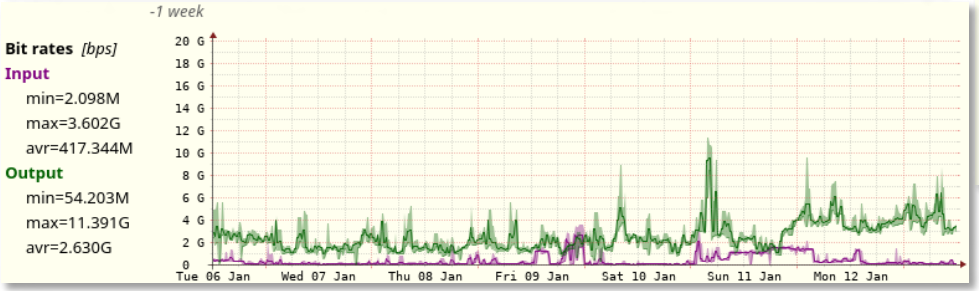


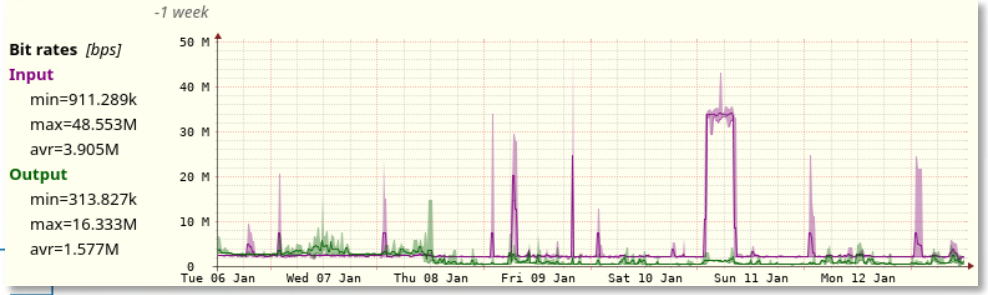
cesnet

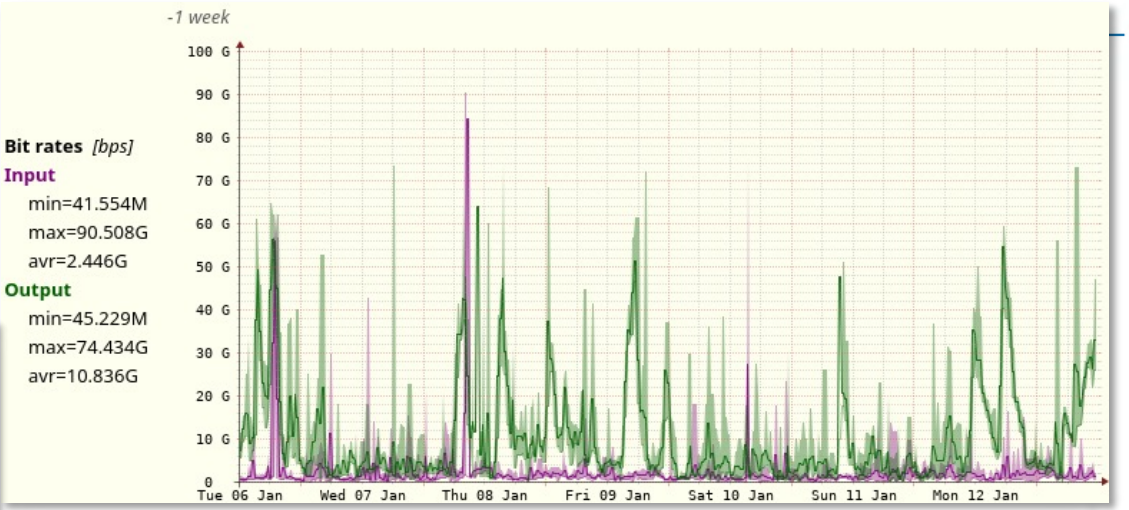
Automatizovaná obrana sítě

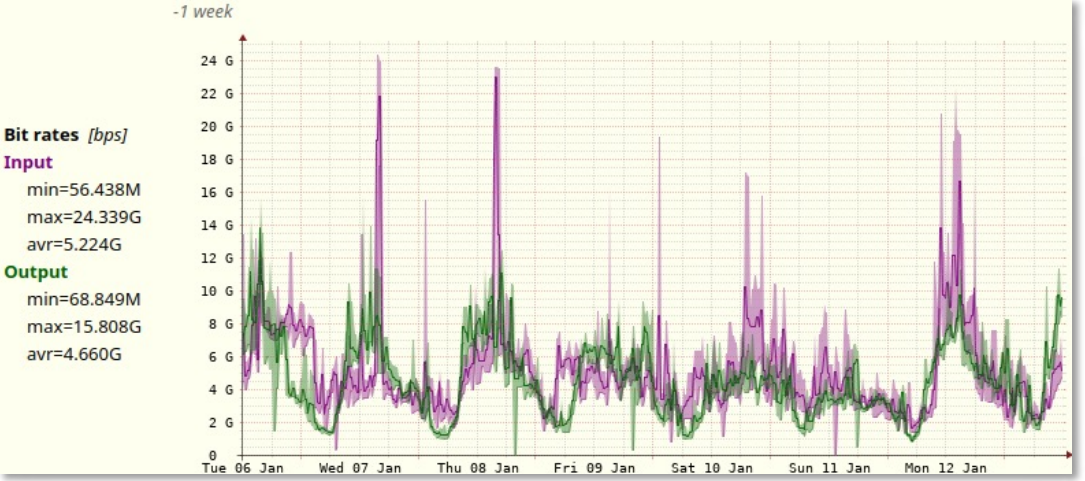
Evoluce architektury

- velké provozní rozdíly
- malý podíl deterministického provozu
- skupiny „podobných“ uživatelů









cesnet

Automatizovaná obrana sítě

Evoluce architektury

- současný model
- „segmentace“

Modularita

- autonomie síťových entit
- vícestupňová obrana

Flexibilita

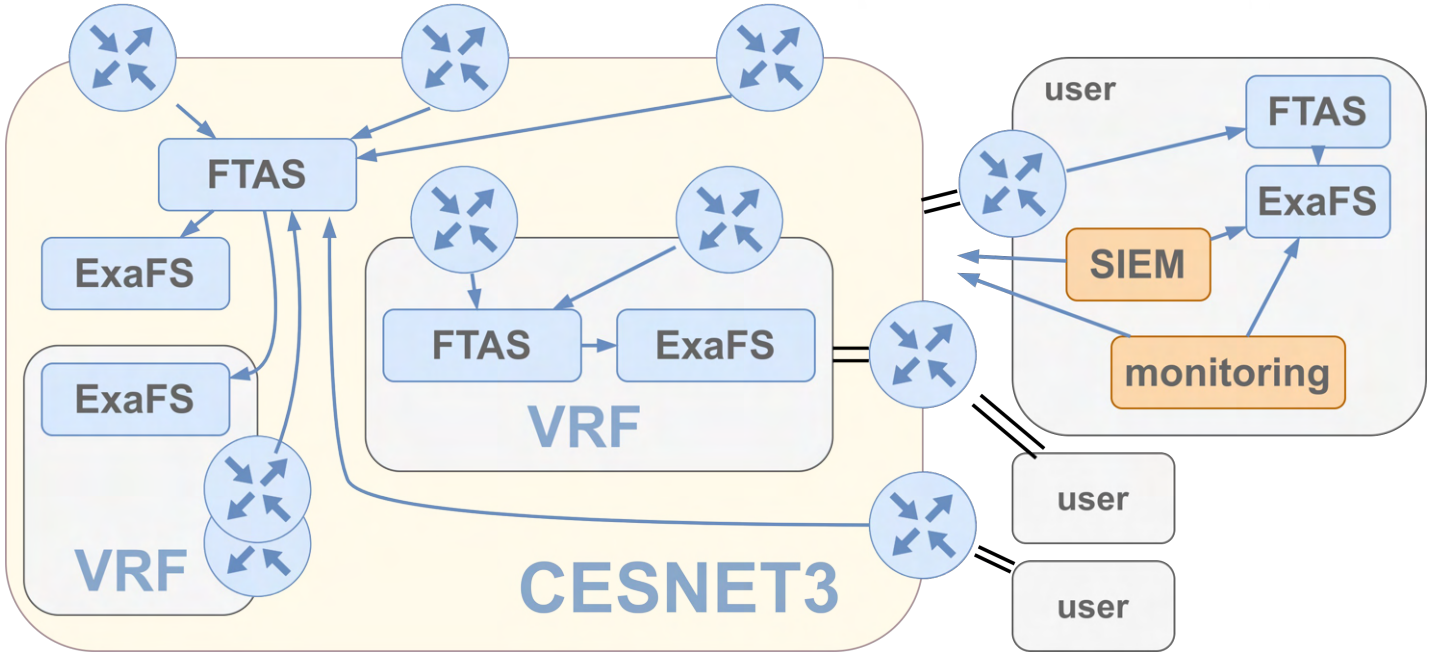
- libovolné vazby mezi prvky obrany

Hybridní model řízení

- e-infrastruktura
- uživatelé

VRF

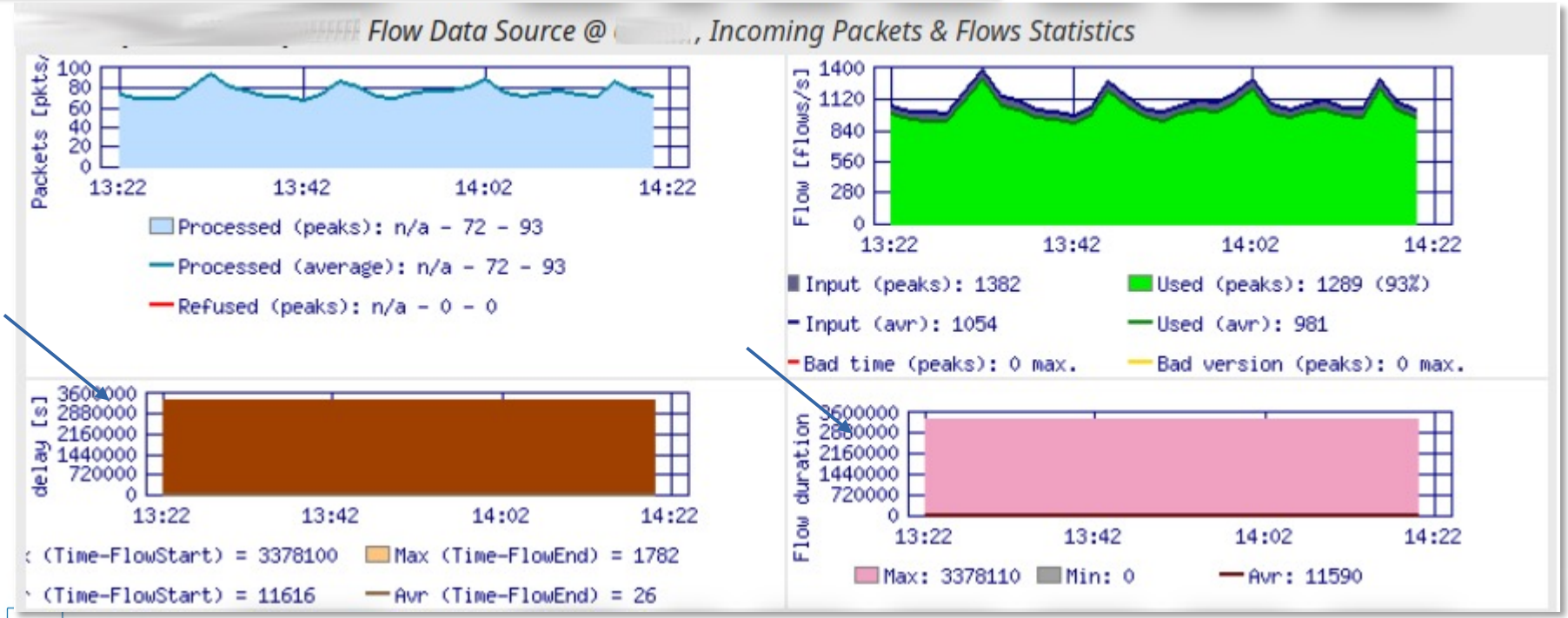
- síť v síti
- **špatné pro jednoho → špatné pro všechny**



Na co myslet, úskalí..

NetFlow

- potřebujeme “semi-real-time“ data..

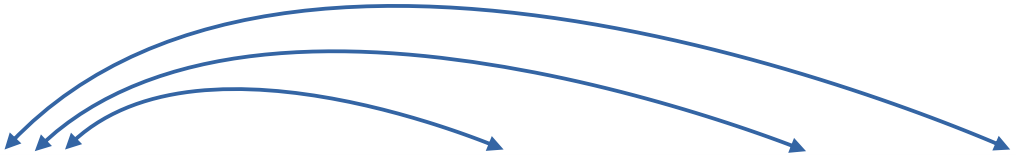


cesnet

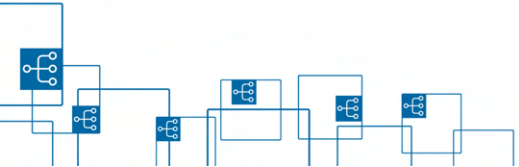
Na co myslet, úskalí..

NetFlow

- potřebujeme „relativně přesná“ data…



Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	TCP-flags	Bytes-measured	Pkts-measured	Avr-Pkt-Length	Flow-Cnt
79.x.x.x	147.x.x.x	tcp (6)	https (443)	63612	syn(2)	15.164 MB	11.907 Kp	1273.55	1
143.x.x.x	147.x.x.x	tcp (6)	17340	http (80)	syn(2)	4.279 MB	2.892 Kp	1479.60	1
2.x.x.x	147.x.x.x	tcp (6)	https (443)	49164	syn(2)	2.488 MB	1.955 Kp	1272.60	1
147.x.x.x	147.x.x.x	tcp (6)	17340	http (80)	syn(2)	1.452 MB	1.155 Kp	1257.16	1
168.x.x.x	147.x.x.x	tcp (6)	https (443)	50535	syn(2)	1.083 MB	785.000 p	1379.76	1



cesnet

Na co myslet, úskalí..

NetFlow a detekce

- **sampling & extrapolace**
- potřebujeme „reálné“ hodnoty ? → **detekce na bázi extrapolace ?**
  - kdy dává smysl ?
  - co [ne]extrapolovat ? ..packets, octets vs. flow-count ?
  - přemýšlet, přemýšlet ..implicitní false positives ;-(
- **testovat** „pokud je to možné“ → dry run / testovací adresy / „bezpečná“ pravidla
- **živý organismus, průběžné ladění**

False positives ..?

Zadávání pravidel pro regulaci

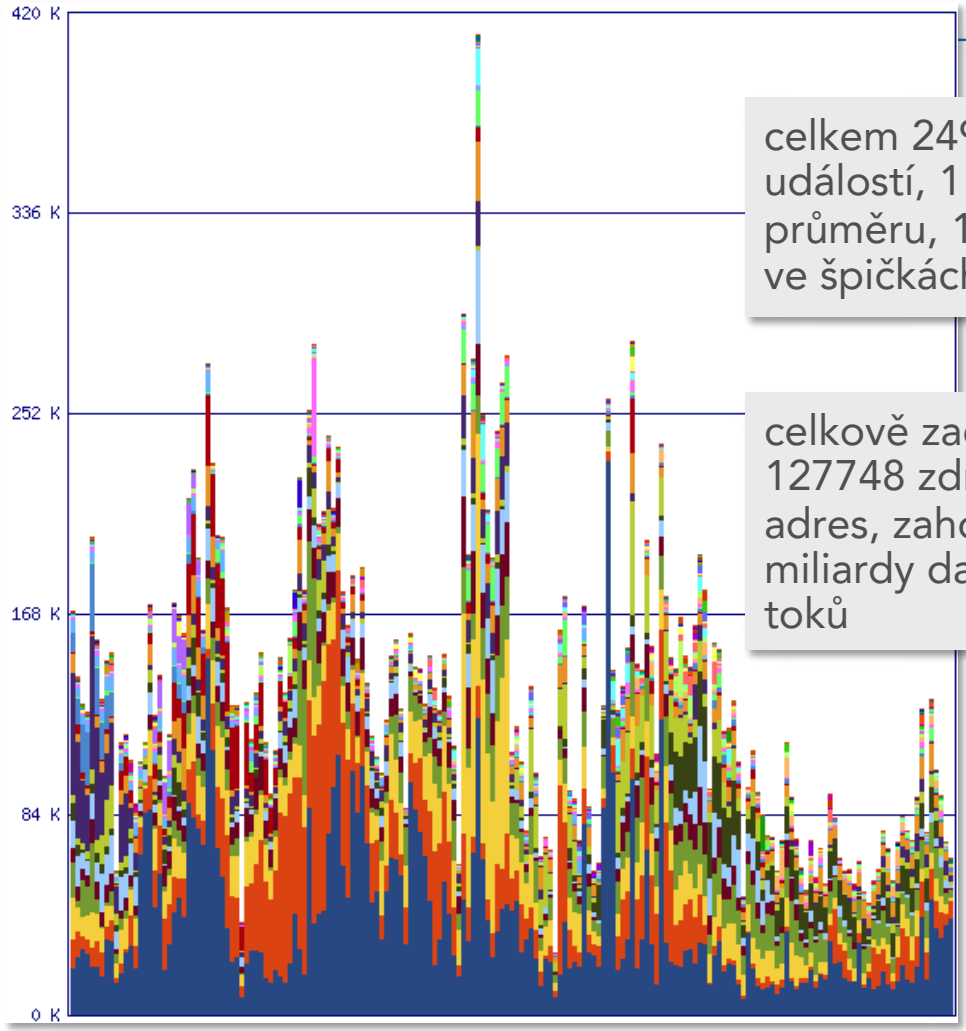
- počet pravidel, spotřeba zdrojů
- vícenásobné ošetření stejného jevu / různými způsoby ~ FlowSpec, RTBH
- kontrola existujících pravidel - není tam už „silnější“ ..?
- kombinatorika pravidel - „rozlomení“ less-specific na části...

cesnet

Jak to vypadá v realitě ?

1. stupeň – celá síť

- **dopad na všechny uživatele**
- **kompromisní citlivost a agresivita detektorů**
- ukázka průběhu detekcí (zdroje)
- 12 měsíců
- 1 hodnota v grafu = počet událostí za 48h
- co má vliv na počet detekcí ?



celkem 24907186 událostí, 1 za 1.3s v průměru, 1 za 0.43s ve špičkách

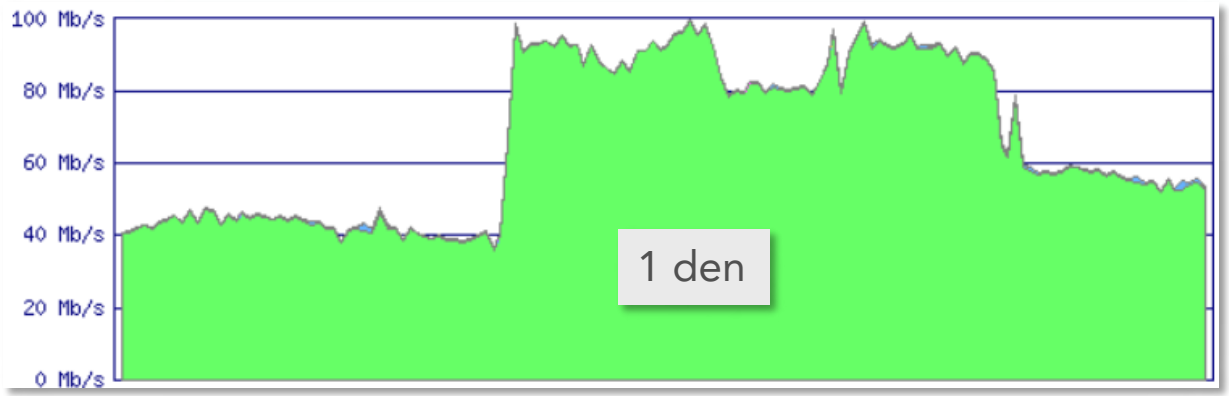
celkově zachyceno 127748 zdrojových adres, zahozeno 2.2 miliardy datových toků

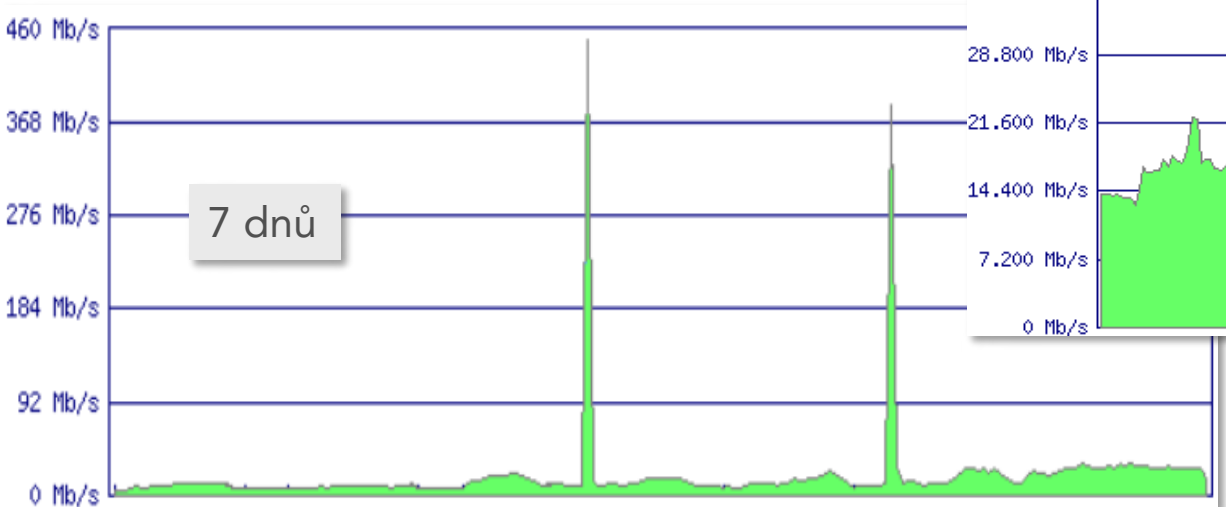
cesnet

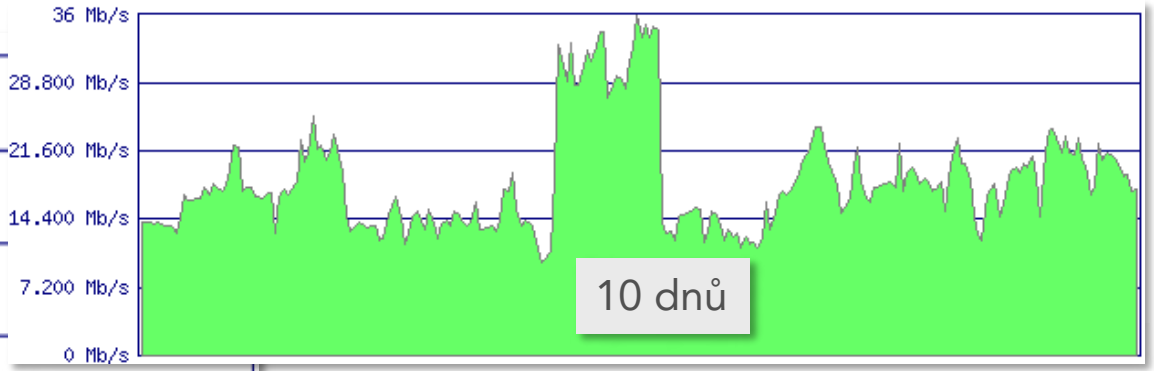
Jak to vypadá v realitě ?

1. stupeň – celá síť

- různé náhodné ukázky průběhů zahozeného provozu





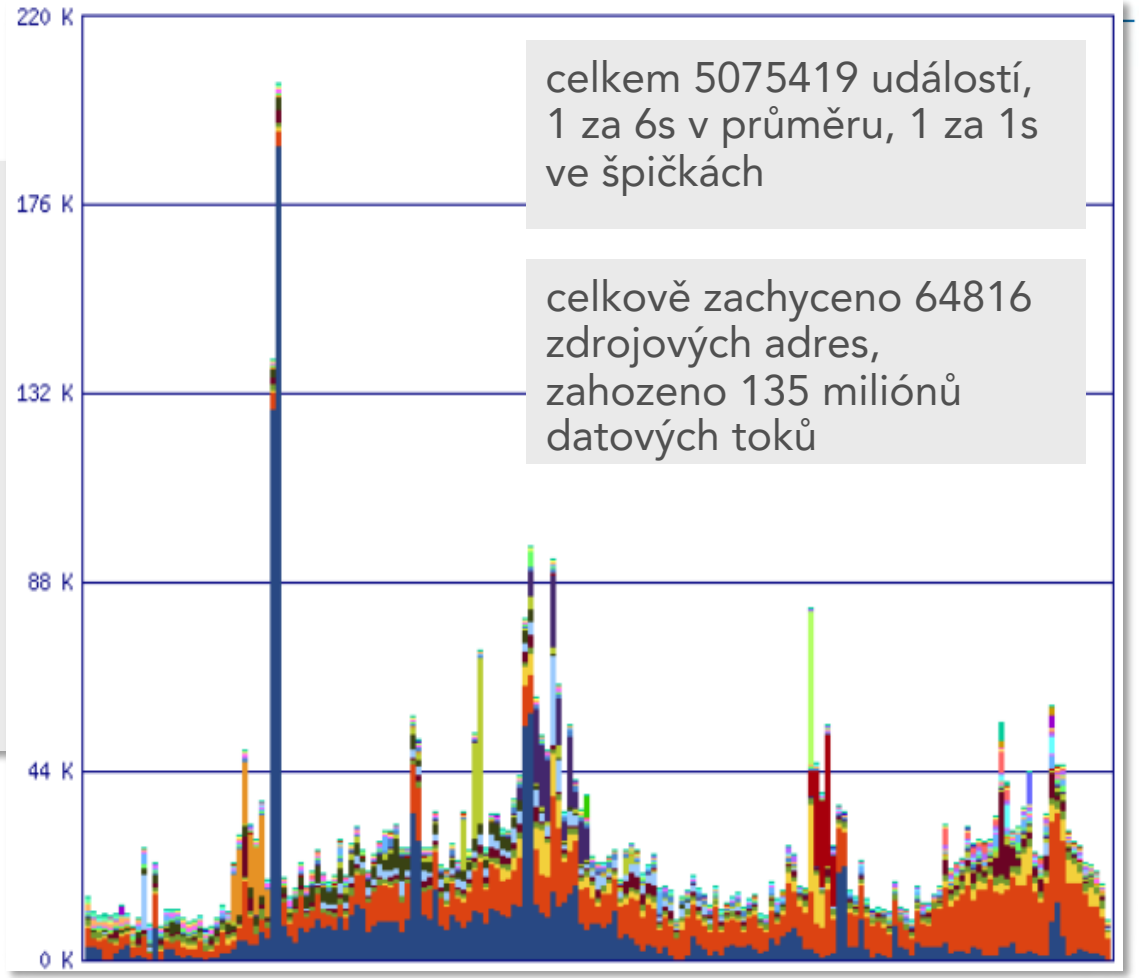


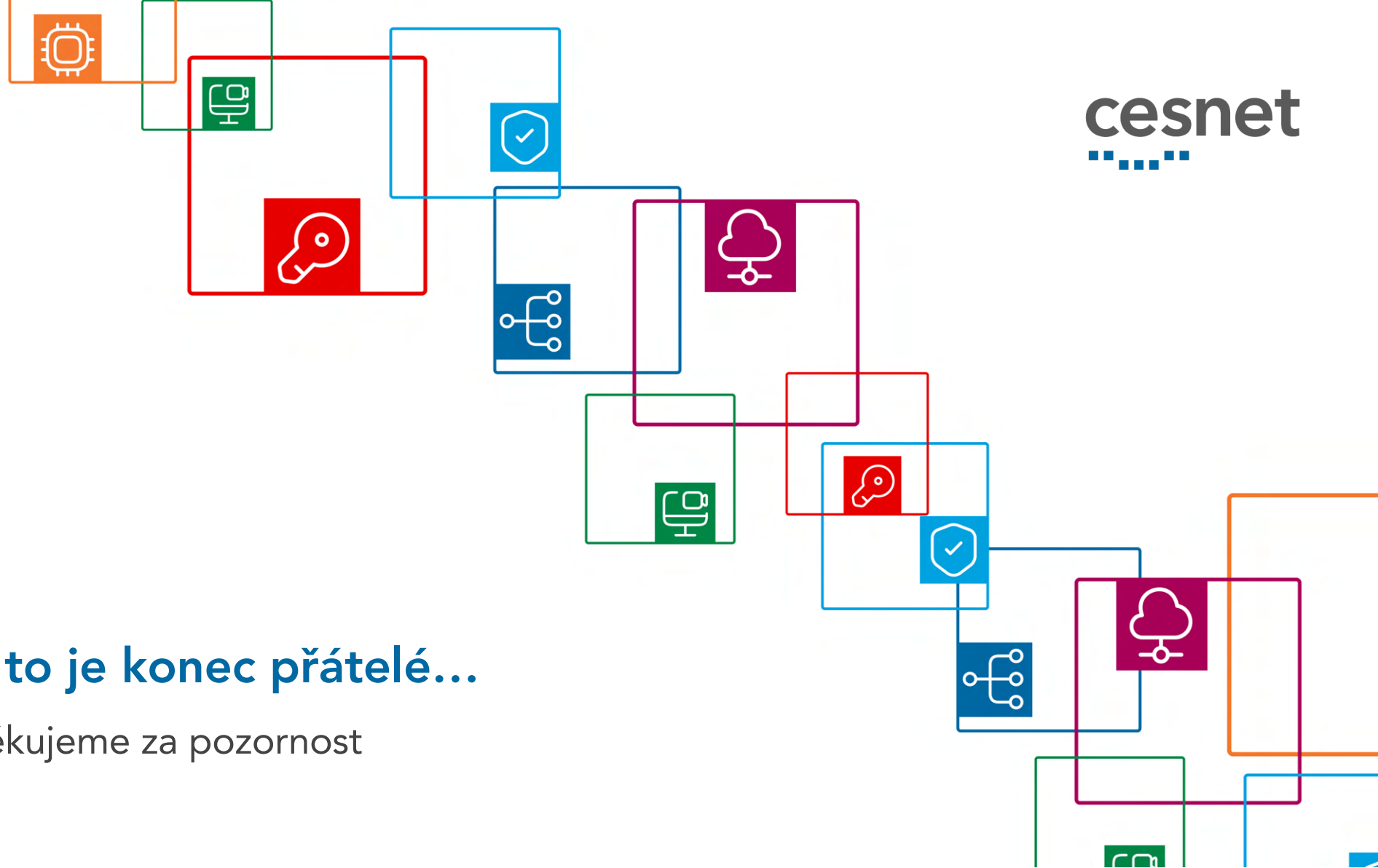
cesnet

Jak to vypadá v realitě ?

2. stupeň – VRF

- **„dočištění“ toho, co prošlo 1. stupněm**
- **vyšší citlivost a agresivita**
- cílené nastavení na potřeby skupiny
- 12 měsíců
- 1 hodnota v grafu = počet událostí za 48h





cesnet

A to je konec přátelé…

Děkujeme za pozornost