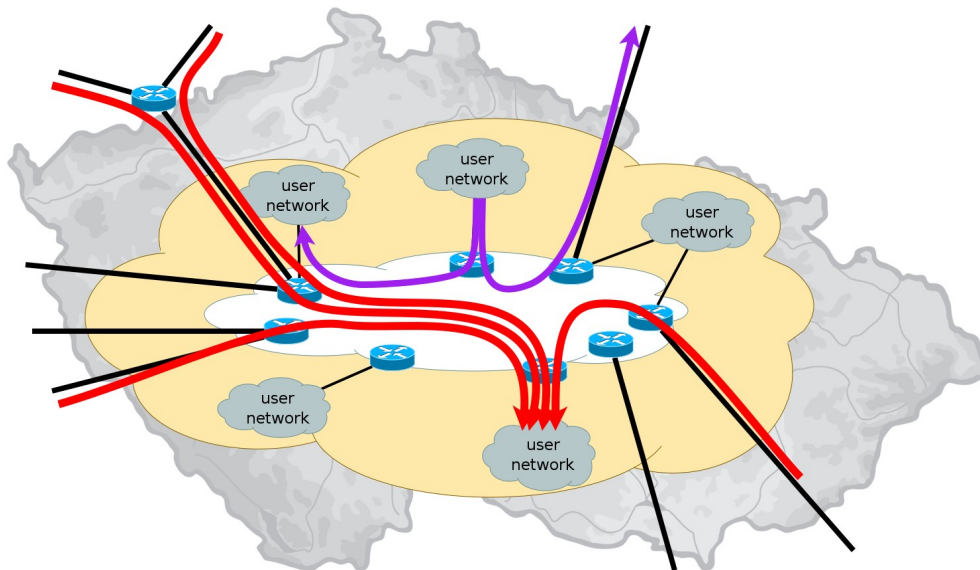


Bezpečnostní prvky síťové infrastruktury

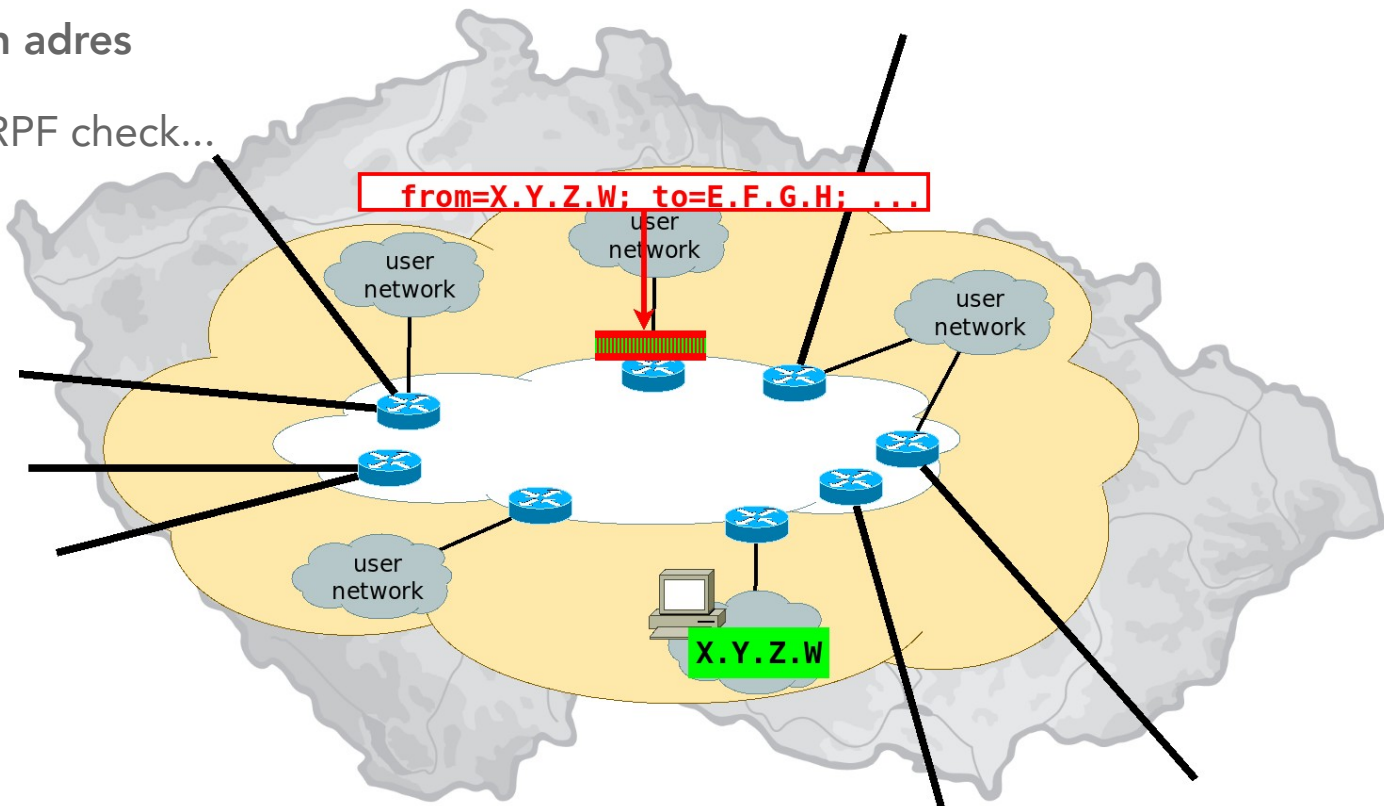


- zamezit zahlcení
 - páteře
 - uživatelských přípojek
 - *externích propojení*
- **eliminovat nelegitimní provoz v síti**
- ošetřit/regulovat anomálie v provozu
- ...
- pomoc při problémech v koncových sítích na úrovni transportu v síti e-infrastruktury
- *události mající původ „vně AS“ vs. „uvnitř AS“ ?*



- **access listy** ~ filtry provozu
- řízený přístup k jednotlivým částem sítě
 - správa sítě vs. běžný provoz, CPP
 - účelově dedikované části sítě
- eliminace invalidní adresace v daném síťovém kontextu

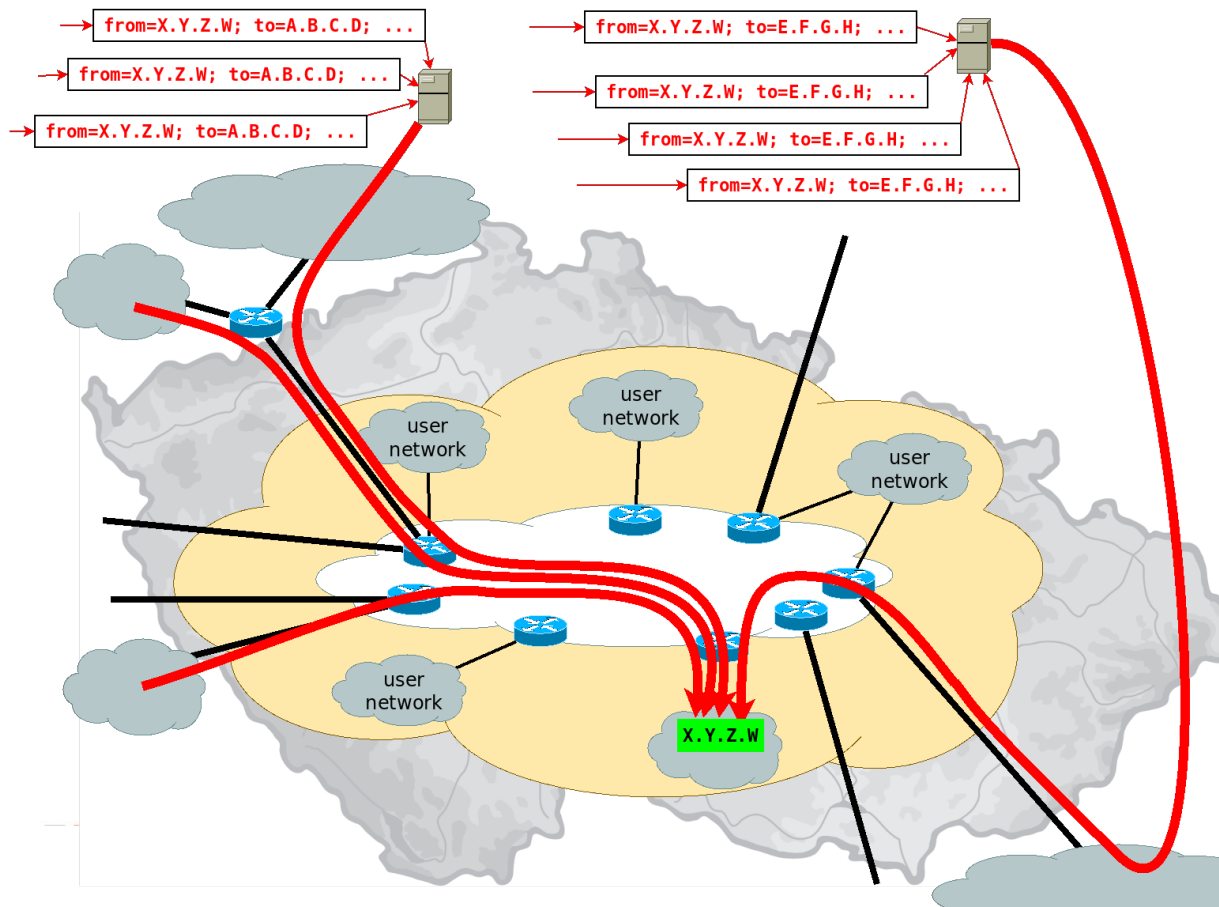
- kontrola zdrojových adres
- BCP-38, RFC2827, RPF check...
- nativní funkce
- + statické filtry



- kontrola zdrojových adres

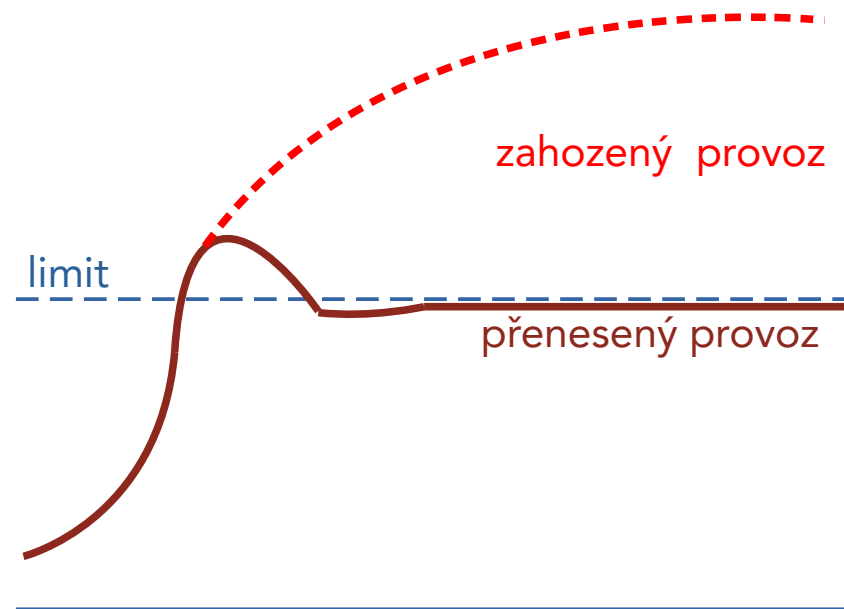
- ...absence dostatečné míry ošetření v globálním měřítku ?

→ snadno realizovatelné specifické DoS

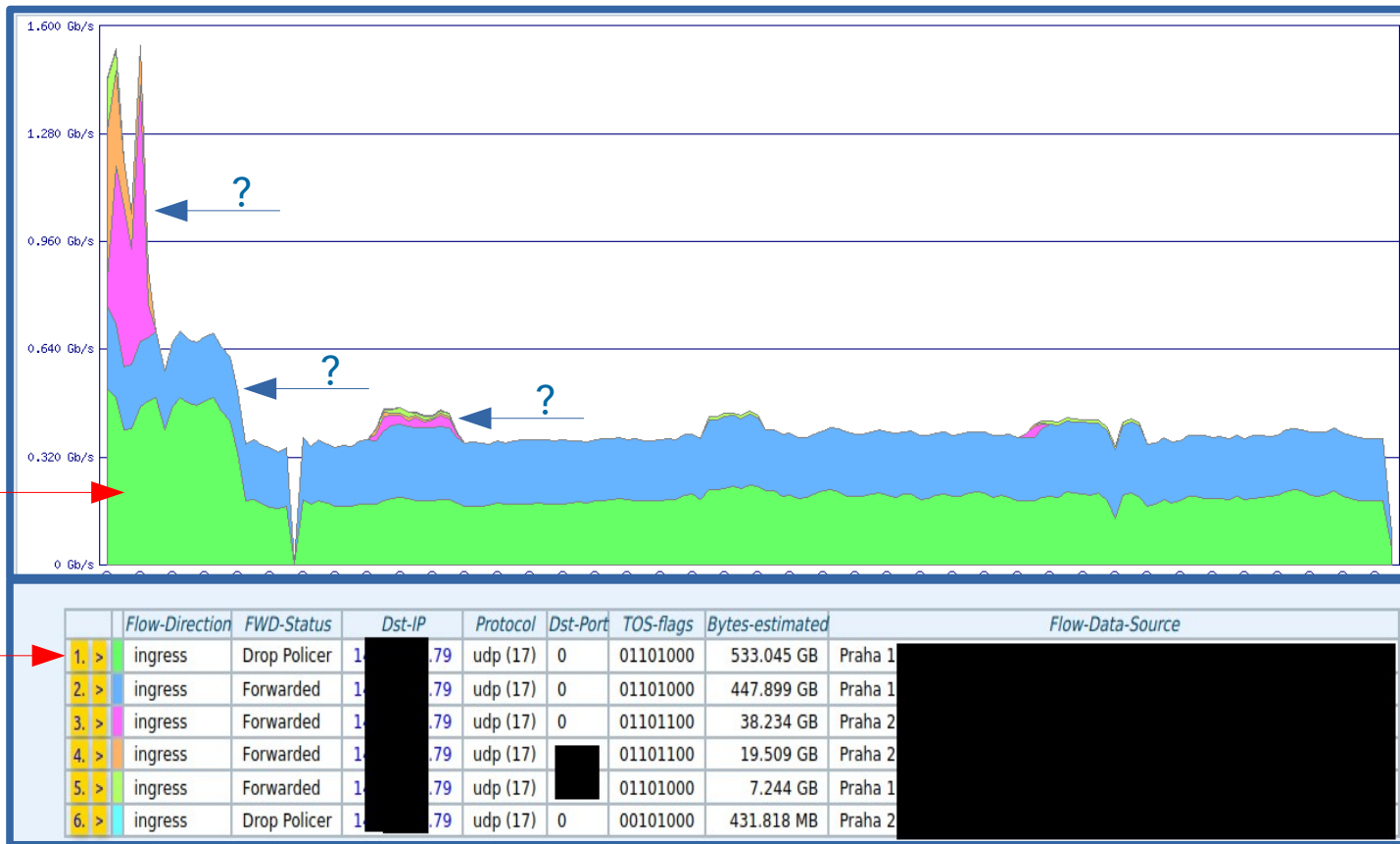


- Resource Public Key Infrastructure – RPKI
- BGP výměna směrovacích informací
 - kontola validity prefixů (*~adresních rozsahů, bloků*)
 - zahození invalidních prefixů
 - důvěryhodnost směrování
 - zabraňuje „únosu prefixů“

- policing na perimetru sítě
- profily pro specifický provoz
 - typ provozu
 - granularita rozhodování
 - limity
- průběžný update
 - nově identifikované útoky
 - diskuze s uživateli
 - upgrady kapacit

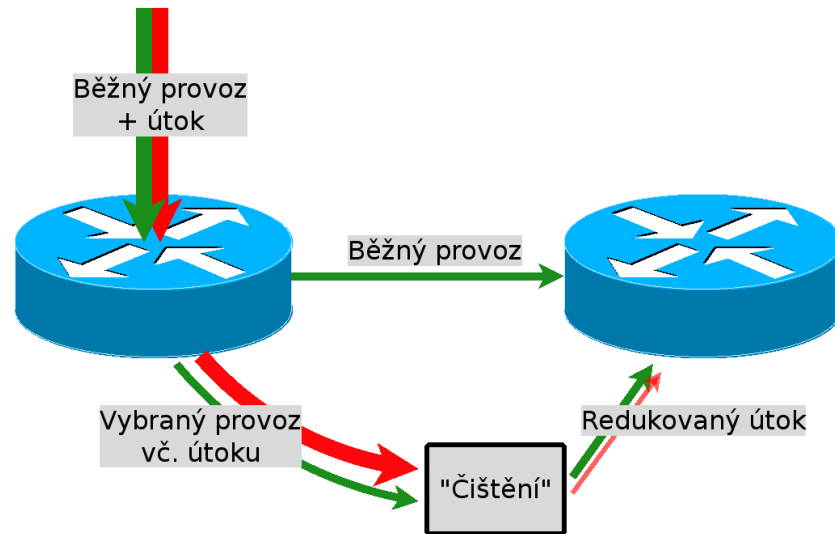


- policing na perimetru sítě
- ukázka funkce

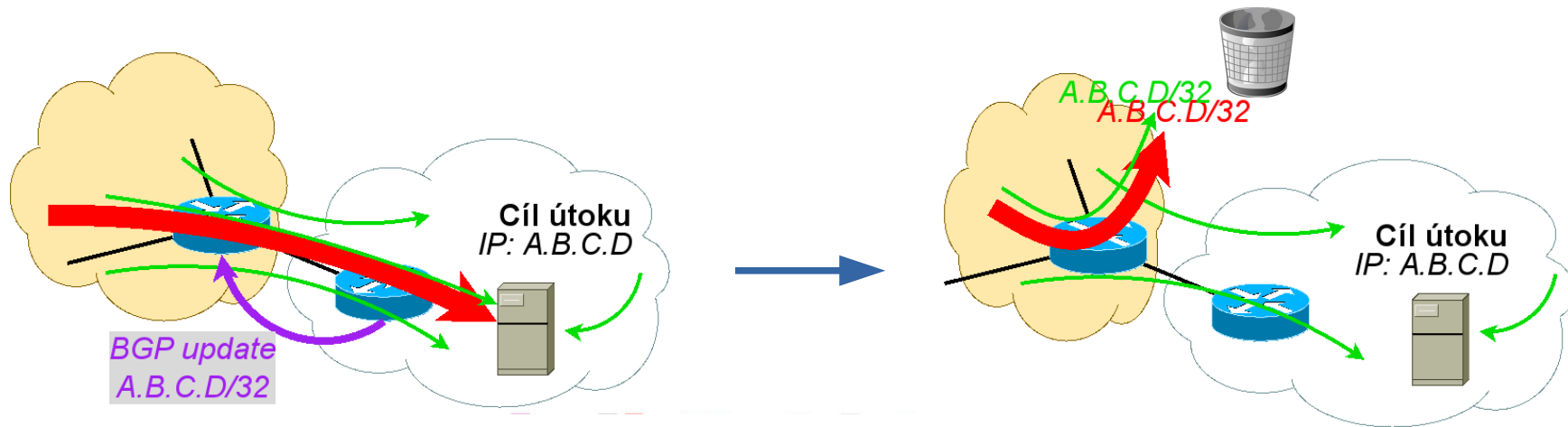


- rozbor vysvětlení vlivu ostatních prvků obrany – 22.4. „Bezpečnost“

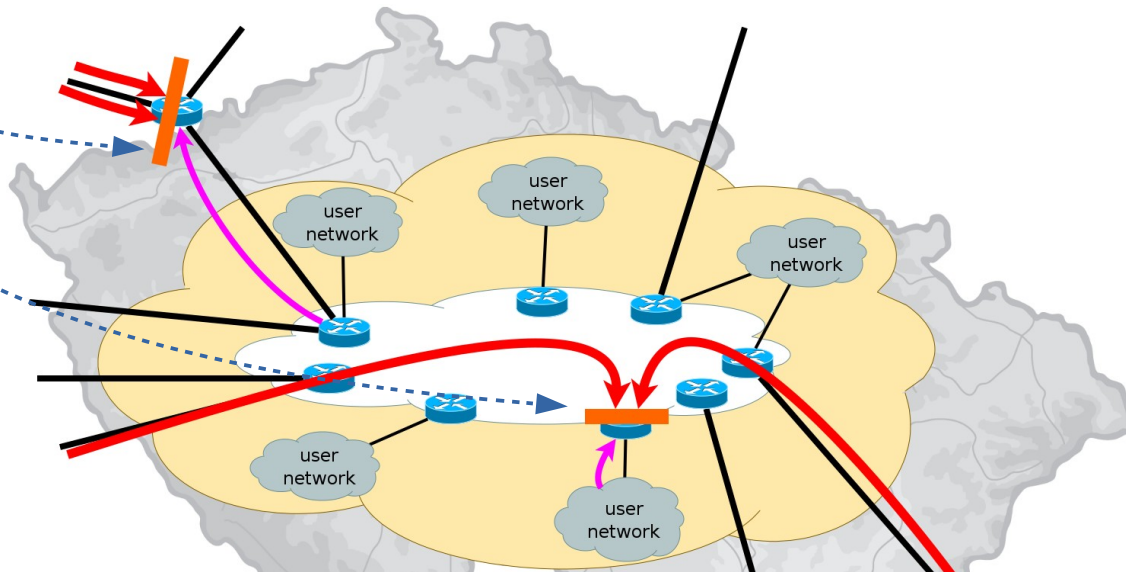
- DoS protector
- in-house řešení na bázi prog. HW
- heuristiky pro řešení typických DoS



- Remotely Triggered Black Hole - RTBH
- zahození provozu pro cílový prefix v předchozí síti (z hlediska směru přenosu)



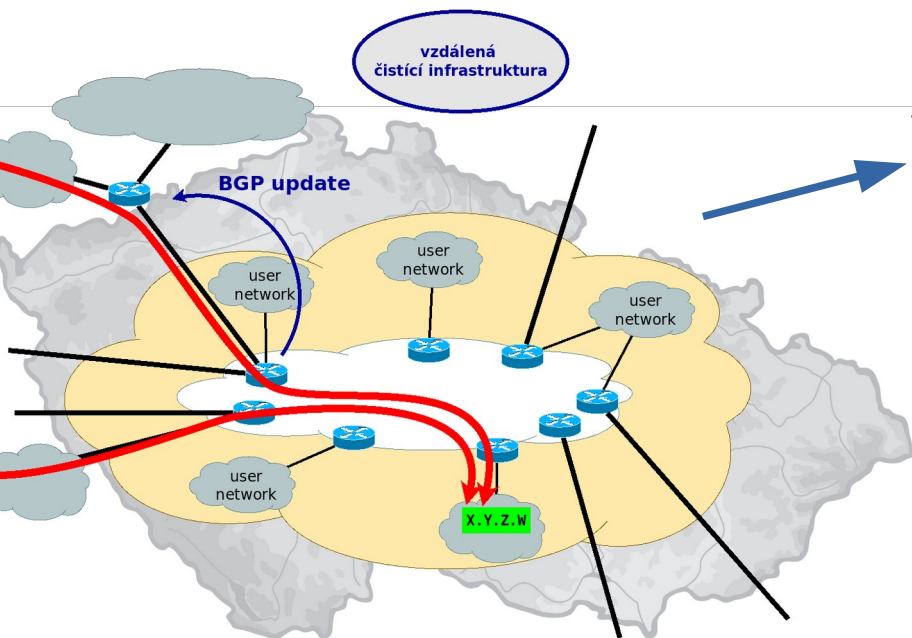
spolupráce s externími partnery, kde je to v principu možné



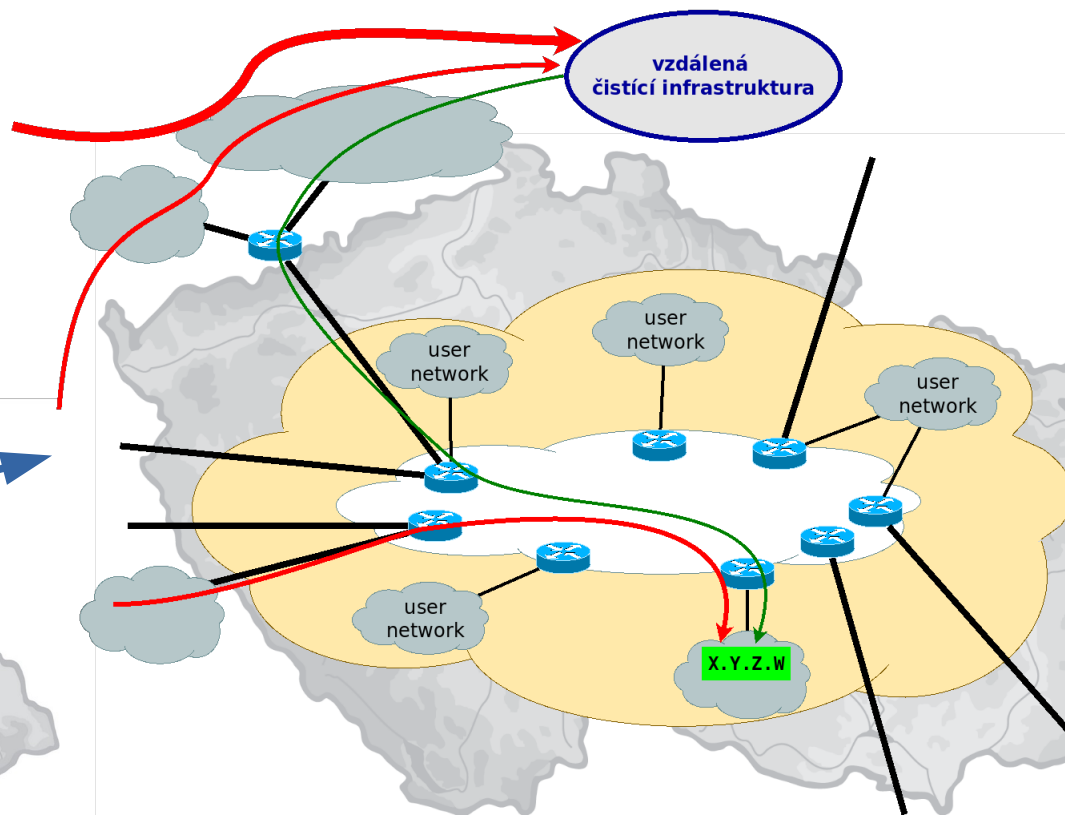
- **BGP FlowSpec**
- rozšíření BGP
- jemnější specifikace konkrétních toků na základě širší sady parametrů
 - prefixy, protokol, porty, ICMP (type, code), TCP flags, Pktlen, DSCP, Fragment encoding
- pravidla pro regulaci
 - rate (vč, zahození), redirect, marking, action
- ~ *ad-hoc nastavení profilu pro doručování specifického provozu*

- **vzdálené čištění provozu**
- před vstupem do e-infrastruktury → *mj. ochrana externích propojek*
- ve spolupráci s poskytovatelem tranzitu
- na základě specifické směrovací informace
 - přesměrování příslušného provozu již v síti Tier-1 operátora do čistící infrastruktury
 - potenciální vliv i na ostatní příchozí směry
 - návrat vyčištěného provozu

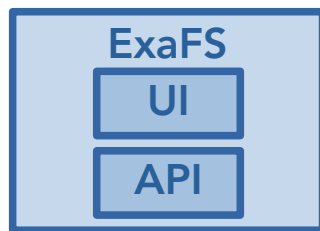
- vzdálené čištění provozu



Prvky obrany



- ExaFS
- nástroj na řízení, ExaBGP
- RTBH, BGP FlowSpec, vzdálené čištění,..
- UI, API, strukturovaná přístupová práva



síťová část e-infrastruktury

/ ExaFS_0.4.9 Add IPv4 Add IPv6 Add RTBH API Key Logged in as FTAS cesnet.cz, role: user, org: Cely svet

Active IPv4 rules

IPv4 IPv6 RTBH Search... Active Expired All

Active IPv4 rules that you can modify

Source address	Source port	Dest. address	Dest. port	Protocol	Expires	Action	Flags	User	Edit	
[redacted] 19.75 / 32			3702	udp	2022/01/31 10:00	Discard		[redacted]	[edit] [delete] [info]	☐
[redacted] 0.32 / 32			389	udp	2022/01/31 10:00	Discard		[redacted]	[edit] [delete] [info]	☐
[redacted] 27 / 32			623	udp	2021/03/01 10:00	Discard		[redacted]	[edit] [delete] [info]	☐

/ ExaFS_0.4.9 Add IPv4 Add IPv6 Add RTBH API Key Logged in as FTAS cesnet.cz, role: user, org: Cely svet

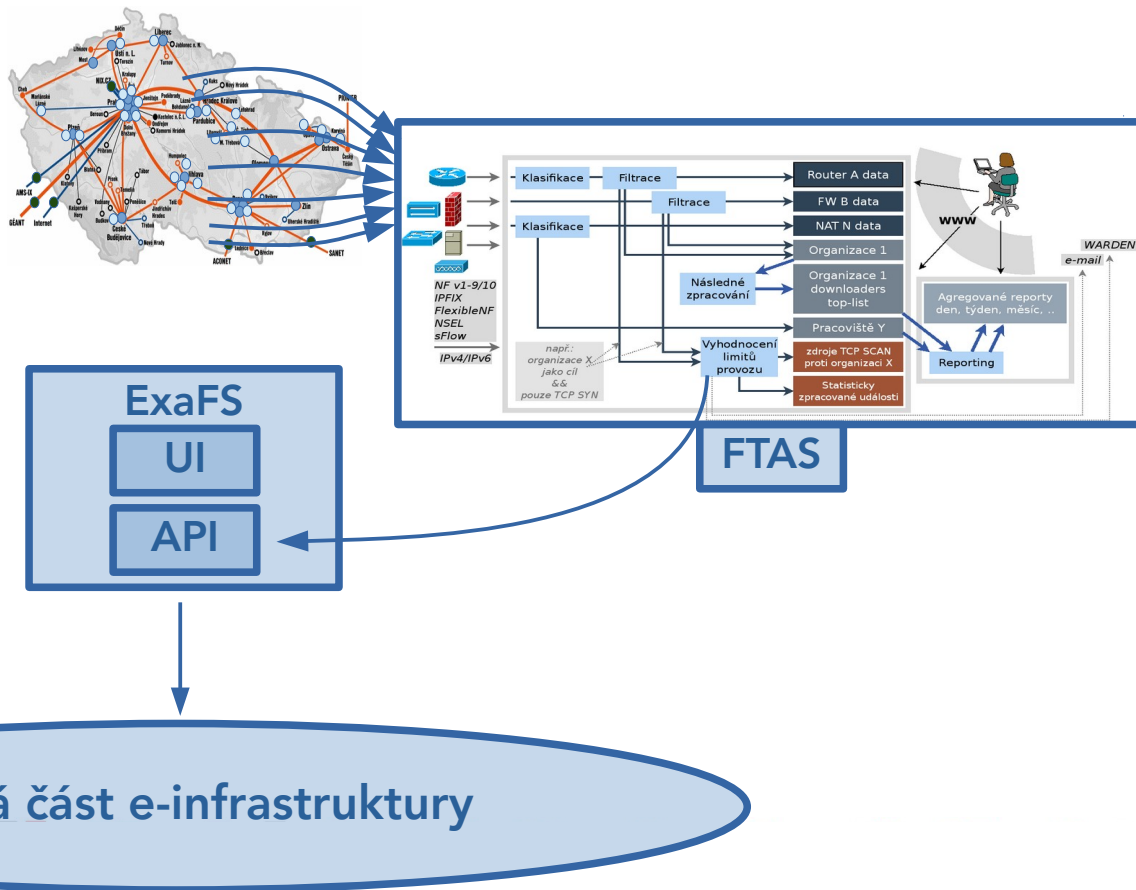
Active RTBH rules

IPv4 IPv6 RTBH Search... Active Expired All

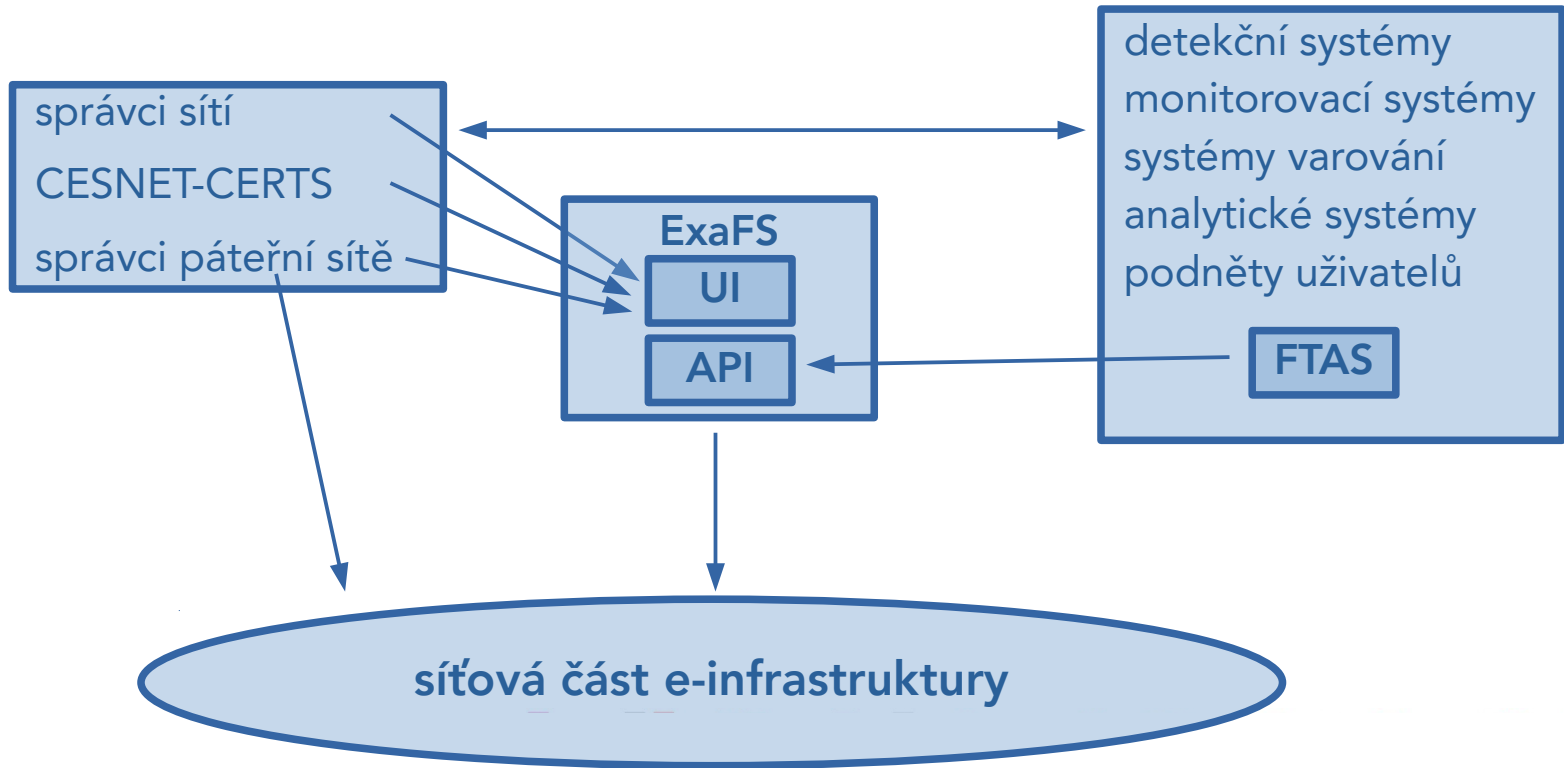
Active RTBH rules that you can modify

IP address (v4 or v6)	Community	Expires	User	Edit	
[redacted] 208 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] 53 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] 82 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] 213 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] 241 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] 210 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐
[redacted] 162 / 32	RTBH CESNET only	2021/02/08 09:10	FTAS	[edit] [delete] [info]	☐

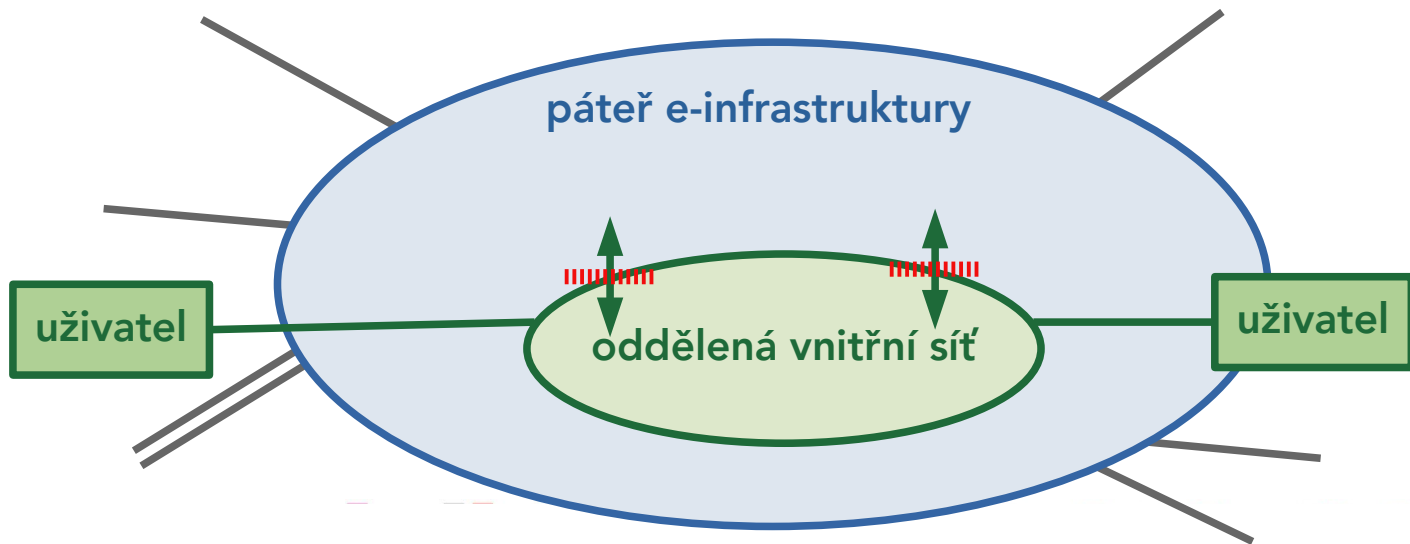
- řada systémů pro sledování infrastruktury a provozu sítě, služeb
- příklad - FTAS
- flow-based monitoring
- plošný sběr z páteře
- zpracování, uchování, vizualizace
- detekce událostí, notifikace
- přímé řízení ExaFS



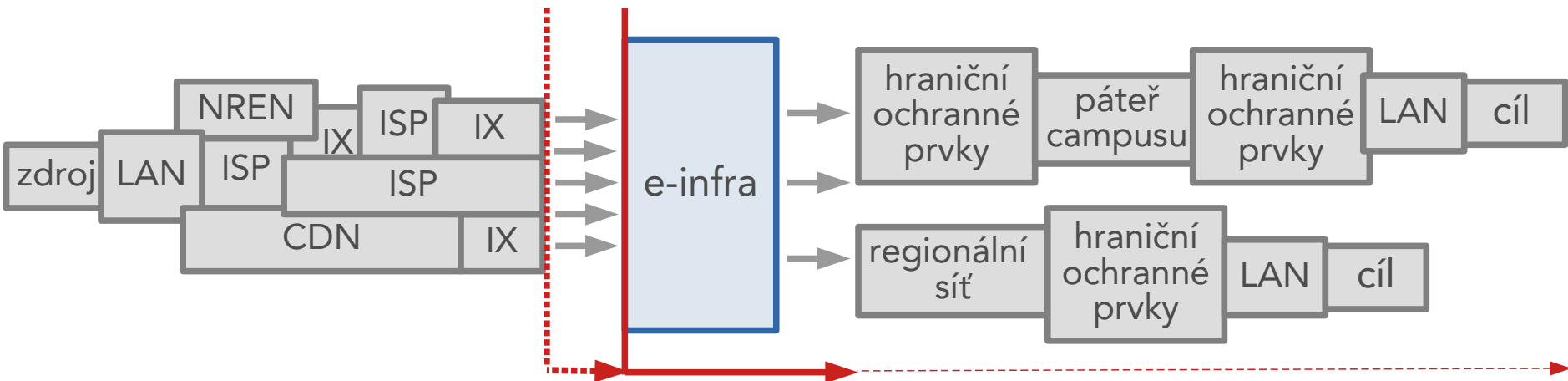
- celkové rámcové schéma řízení a rozhodování



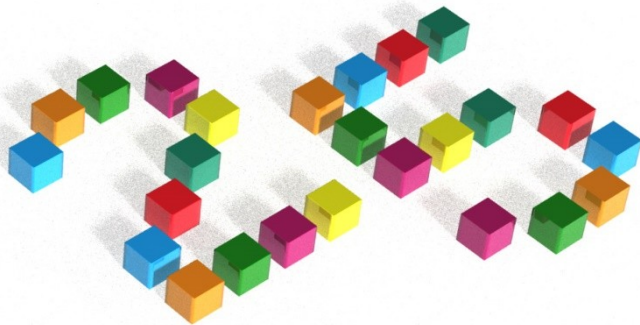
- komplexnější řešení pro specifickou komunitu ~ iniciativa hSOC
- „sít' v síti“, dvoustupňová ochrana
- samostatné instance relevantních prvků na vnitřních propojích



- jedna část přenosového řetězce
- limity „z podstaty“ ~ sdílené transportní prostředí, pouze určité typy jevů
- možnosti dány architekturou, nastavením, monitoringem, rozhodovací schopností
- nelze rezignovat na ošetření navazujících částí řetězce přenosu dat



...bezpečnost nelze „outsourcovat“...



Děkuji za pozornost!



Bezpečnostní prvky síťové infrastruktury