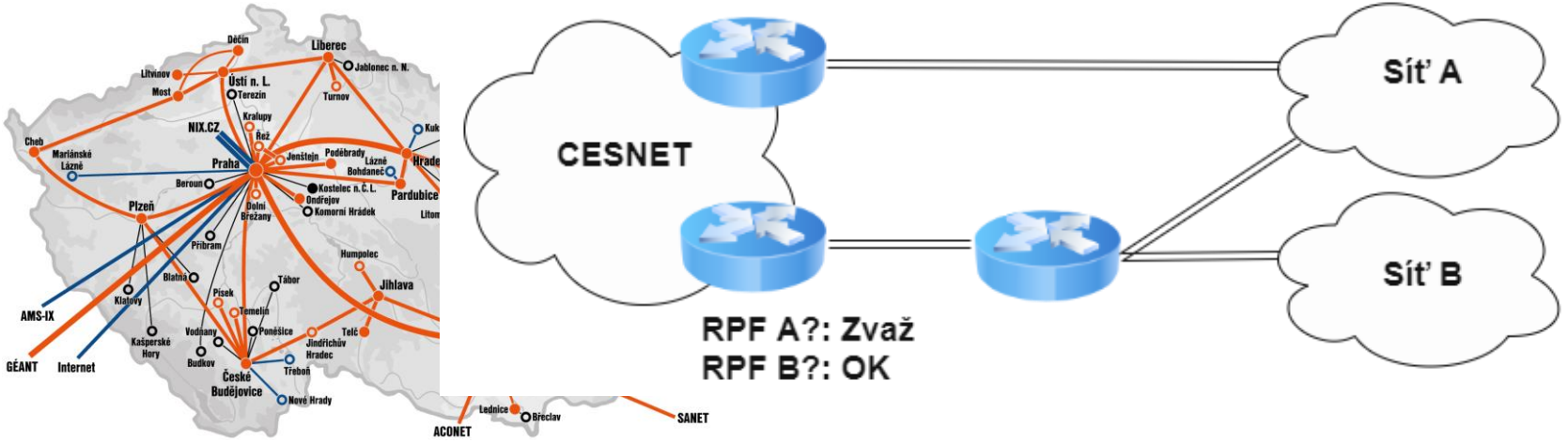
Use-cases z bezpečnostního monitoringu e-infrastruktury CESNET

Monitoring DDoS provozu

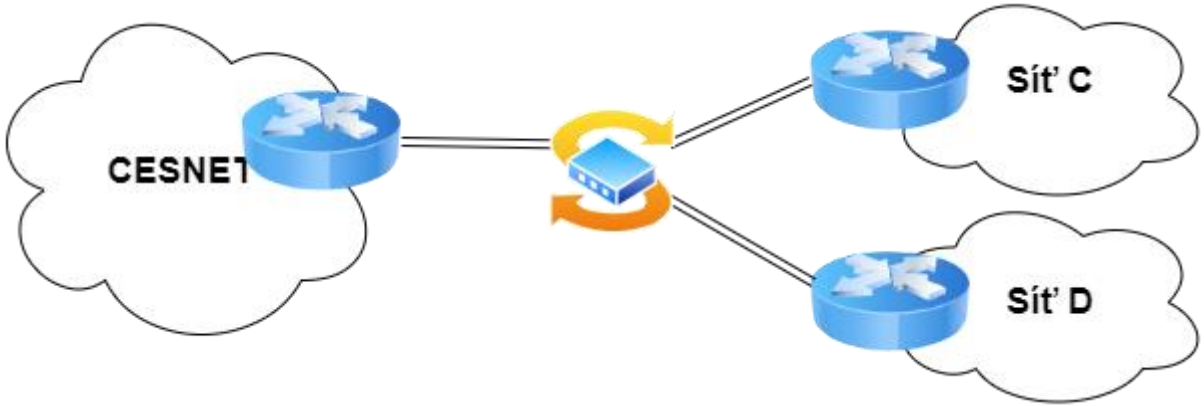
Odkud ty pakety chodí?

- CESNET aplikuje Reverse Path Filtering na hraně své páteřní sítě
- Různá úroveň přísnosti filtrování



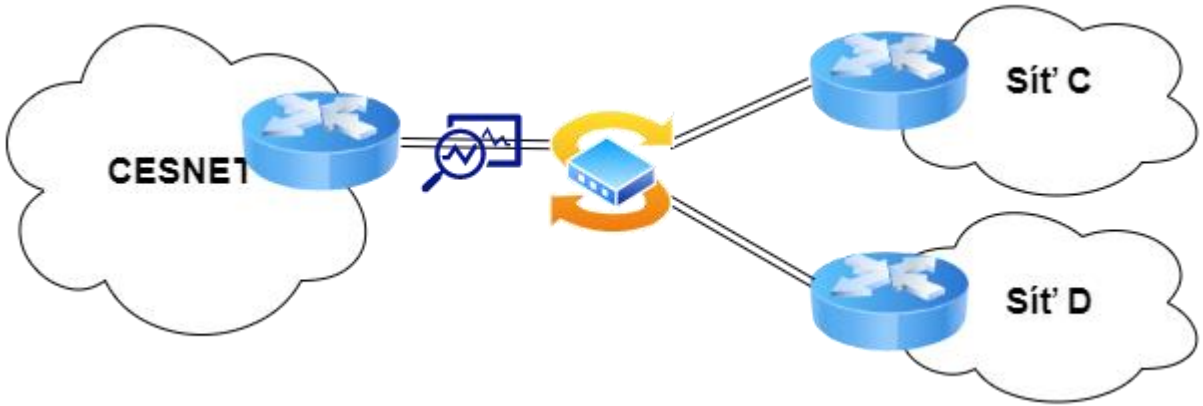
Odkud ty pakety chodí?

- CESNET kromě přímého peeringu je připojen do peeringových uzlů
- Aplikovat RPF na lince do peeringového uzlu je problematičtější
- Obečně je dobré vědět od jakého peering partnera DDoS přichází



Odkud ty pakety chodí?

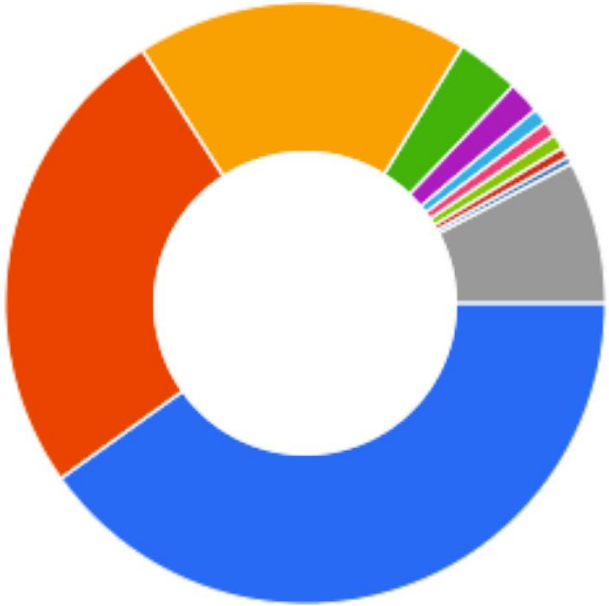
- Je potřeba monitoring provozu na lince do peeringového uzlu, který dovolí zkombinovat L2 a L3 pohled



Odkud ty pakety chodí?

- Díky flexibilní monitorovací infrastruktuře můžeme monitorovat zdrojové MAC adresy, abychom zjistili protistranu z podezřelým provozem

ZDROJOVÁ MAC ADRESA NA VSTUPU	TOKY	VSTUPNÍ PAKETY	BAJTY NA VSTUPU
d2:cf:40	18.87 M (40.1%)	20.13 M (7.4%)	977.74 MB (0.5%)
a:40:00	12.12 M (25.7%)	12.72 M (4.7%)	819.89 MB (0.4%)
ad:6f:c1	8.41 M (17.9%)	8.66 M (3.2%)	334.63 MB (0.2%)
7:40:5d	1.6 M (3.4%)	3.83 M (1.4%)	1.91 GB (0.9%)
fb:56:0a	832.79 K (1.8%)	14.2 M (5.3%)	7.9 GB (3.9%)



Data pro incident handling

S kým ta stanice komunikovala?

- Organizace kritické infrastruktury připojená přes CESNET byla napadena ransomwarem
- Správce organizace potřeboval dohledat komunikaci k určité IP adrese, aby identifikoval možný zdroj napadení
- Směrovače typicky při monitoringu vzorkují a proto nemohou poskytnout dostatečně průkazný materiál
- Díky akcelerovaným měřícím bodům jsme byli schopni poskytnout přesný výpis a statistiky všech komunikací vztahující se k dané IP adrese

Data pro forenzní analýzu

Detekce C&C v DNS a HTTP

- Forenzní laboratoř CESNET analyzovala určitý malware a zjistila, na jakých doménách běží C&C server. Vidíme komunikaci v naší síti?
- Akcelerované měřící body umí exportovat vybrané položky z DNS a HTTP
- Případ 1:
  - C&C = doménové jméno, na kterém běží HTTP server, který by měl botům dávat příkazy
  - Filtr na DNS a HTTP → dotazy z několika adres – identifikace nakažených strojů
    - Spolehlivější než identifikace podle IP adresy
  - Malware komunikuje přes nešifrované HTTP GET požadavky – podařilo se zachytit
  - Analýza ukázala, že od serveru už chodí jen chybové hlášky (asi již neaktivní botnet)

Detekce C&C v DNS a HTTP

- Forenzní laboratoř CESNET analyzovala určitý malware a zjistila, na jakých doménách běží C&C server. Vidíme komunikaci v naší síti?
- Akcelerované měřící body umí exportovat vybrané položky z DNS a HTTP
- Případ 2:
  - Malware komunikující s C&C přes *tor2web* domény (`*.onion.<tld>`)
  - Filtrování DNS provozu → v naší síti dotazy na tyto adresy vidíme.
    - Získáme tak ale jen seznam DNS resolverů, ne nakažených stanic.
  - Komunikace přes HTTP, IP adresy serverů jsou sice různé, ale hlavička „Host:“ vždy obsahuje danou *.onion* doménu ...
  - Filtrování podle HTTP „Host:“ hlavičky → úspěšné odhalení nakažené stanice.

Hlášení pro Warden

Automatické detekce

- Flow data ze sond na perimetru zpracovává open-source systém NEMEA
- Automatická detekce nežádoucí komunikace, např.
  - Komunikace s C&C servery (dle veřejných blacklistů)
  - DDoS útoky, vč. amplifikačních
  - skenování sítě
  - hádání hesel na SSH, HTTPS