Sondy a čistička provozu

Konference e-infrastruktury CESNET

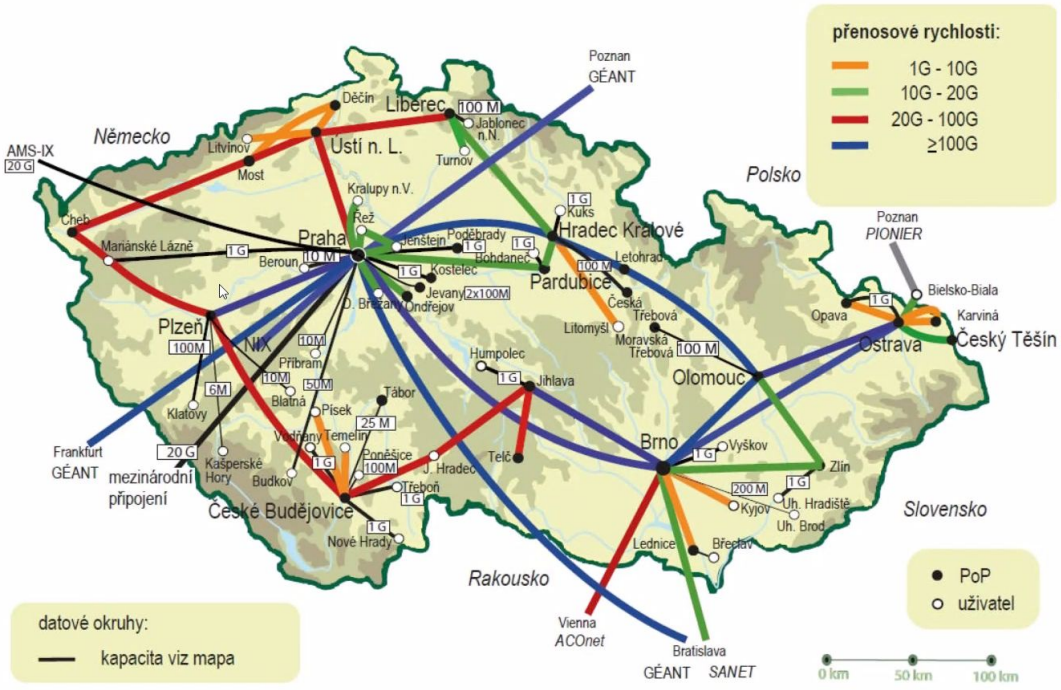
20. dubna 2021

Tomáš Čejka, Jan Kučera

Vysokorychlostní monitorovací sondy

Monitorování perimetru CESNET2

- Hraniční linky spojují e-infrastrukturu se zahraničními sítěmi a komerčním internetem
- Některé linky jsou násobné
- Provozujeme 6 měřících bodů (servery) monitorující perimetr
  - některé body měří více linek najednou



Technologie měřícího bodu

- Vysokorychlostní linky N x 100 Gb/s
- Technologické výzvy
  - propustnost - cíl zpracovat 100% paketů
  - místo/rozměry
    - server je 2U, někde je potřeba provozovat PCIe 2 karty
    - velikost čipu ~ velikost karty
  - chlazení - chladič zabírá celou plochu karty
- Využití FPGA

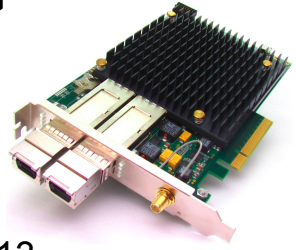
Dostupné/vyvinuté technologie

- Speciální HW pro vysokorychlostní zpracování paketů (COMBO)
  - při >=100 Gb/s a nejkratších paketech je potřeba zpracovat více paketů za takt
- CESNET se podílel na vývoji historicky celosvětově první 100 Gb/s kartě pro HW akcelerované monitorování provozu
- Nyní již máme funkční 200 Gb/s kartu
- Cílíme na 400 Gb/s technologii v příštích několika letech

10G4

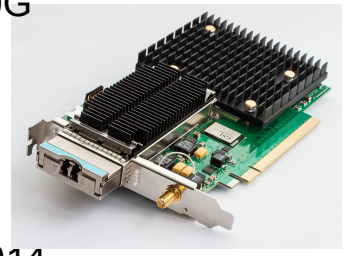
2004

80G



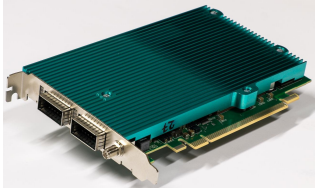
2013

100G



2014

200G



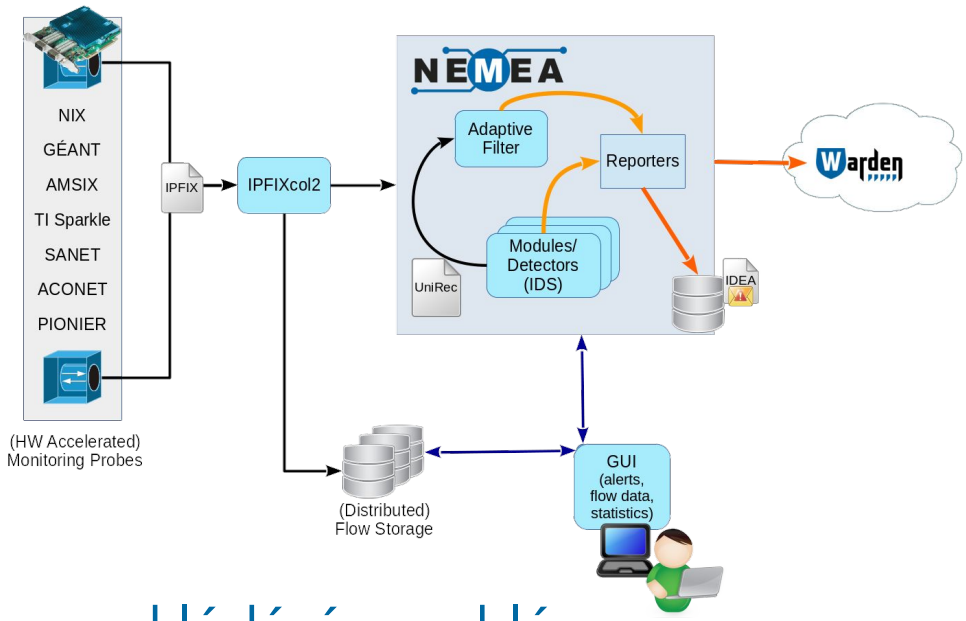
2017

200G2

2019

Monitorovací schopnosti

- Využíváme vlastní infrastrukturu nástrojů postavenou nad IPFIX
- Monitorovací sondy
  - FPGA technologie
  - SW exportér (flowmonexp/ipfixprobe)
- Kolektor
  - ipfixcol2 - open source projekt
- Analýza
  - NEMEA - open source projekt



Provozujeme “distribuovaný kolektor” pro ukládání a rychlé dotazování.

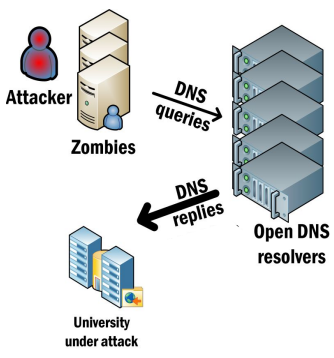
Proč IPFIX?

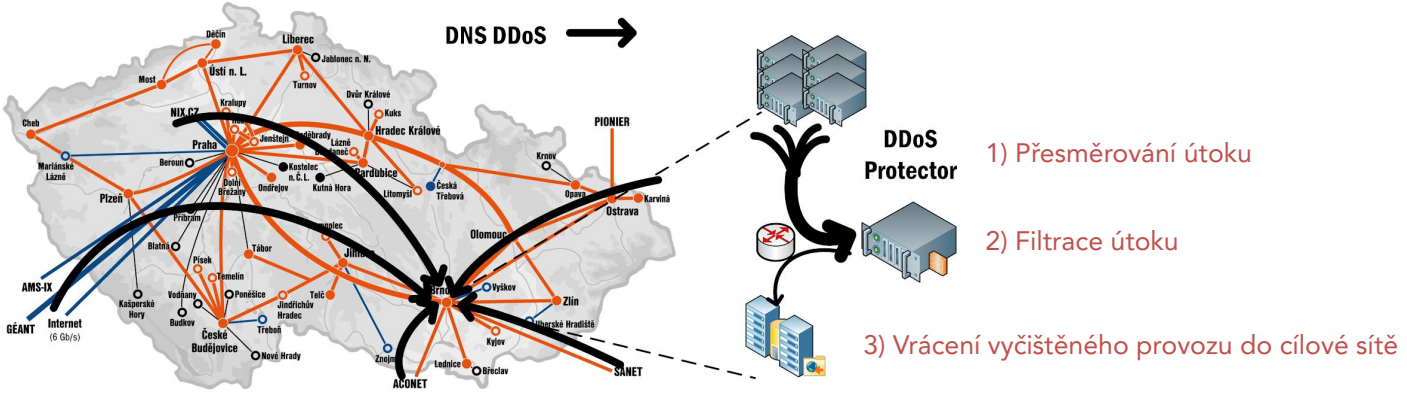
- Měřící body umí extrahovat nešifrované informace z paketů
- Detekce bezpečnostních hrozeb, např.:
  - komunikace s Command&Control servery
  - pokusy o kompromitaci serverů
  - pokusy o zneužití konkr. aplikačních zranitelností
    (v minulosti např. heartbleed, shellshock)
- Rozšířené informace pomáhají s dohledáním zdrojů útoků
  (např. přes peeringová centra)
  nebo získání podrobností k útokům
  (např. memcached amplifikace)
- Tvorba trénovacích a testovacích datových sad

DDoS Protector - čistička provozu

DDoS Protector, čistička provozu

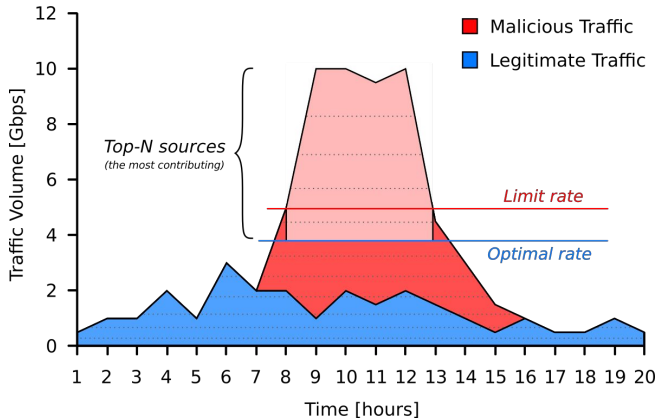
- Systém obrany proti DDoS útokům
  - Postavený nad technologií akceleračních FPGA síťových karet
  - Vytvořen v reakci na útoky na organizace v CESNET, zahlcování kapacity jejich linek
- Dedikované zařízení, přesměrování útoku, vrácení vyčištěného provozu zpět

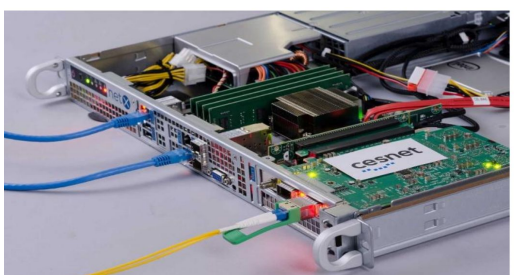




Vlastnosti čističky provozu

- Primárně čistička zaměřena na ochranu konektivity
  - Snaha snížit objem provozu do cílové organizace na zpracovatelnou úroveň
- Alternativa k filtraci na páteřních směrovačích
  - Zdroje vyhrazeny pouze pro čištění
  - Není omezeno specifikací BGP FlowSpec
  - Implementace vlastních algoritmů
  - Umožňuje stavové zpracování
- Propustnost 100 Gb/s i na nejkratší paketech
- Základní typy mitigace:
  - Amplifikační modul
  - SYN Flood modul





Amplifikační modul (heuristika top-N)

- Útoky hrubou silou pomocí odrazu (DNS, NTP, ...)
- Hlídá překročení prahů pro cílové sítě
  - Omezení pro vybraný provoz (threshold, limit)
- Příklad pravidla:

  147.229.0.0/16 protocol UDP port 53
  threshold 1 Gbps limit 500 Mbps
- Při překročení hodnoty threshold:
  - Sleduje množství provozu každého zdroje
  - Omezuje zdroje s největším příspěvkem
  - *top-N* zdrojů až do dosažení limitu

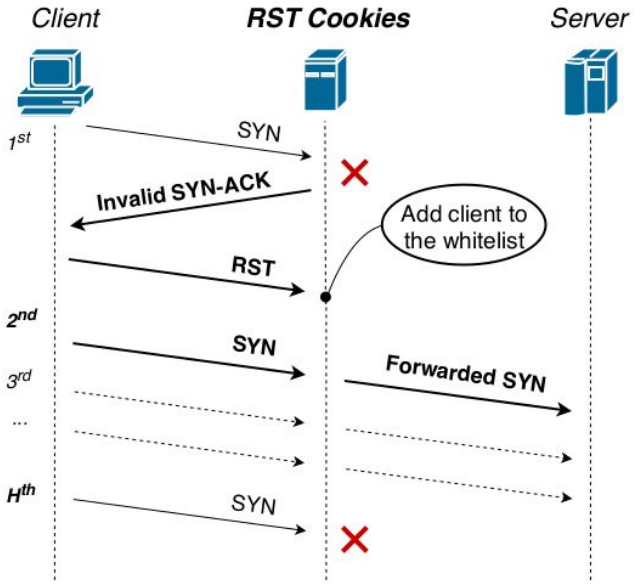
SYN Flood modul

- Heuristiky (SYN Drop, RST Cookies) proti TCP SYN útokům
- Hlídá překročení prahů pro cílové sítě
  - Omezení SYN provozu na vybraných portech
- Příklad pravidla:

  147.229.32.0/24 port 80 threshold 100 kpps
- Při překročení hodnoty threshold:

  A. Počítání statistik SYN a ACK pro každý zdroj a omezování zdrojů SYN bez jiné komunikace

  B. Autentizace klientů algoritmem RST cookies ochrana proti podvrženým IP adresám



Vize budoucnosti

Čistička

- Nasazena v síti CESNET
  - Přesměrování provozu k čištění, nutná však ruční konfigurace pravidel
    - ⇨ Integrace konfigurace čištění do provozních nástrojů infrastruktury
- Vývoj nových heuristik mitigace
  - ⇨ Odvozování pravidel pro mitigaci s využitím strojového učení
  - ⇨ Výzkum adaptivních metod přizpůsobujících se vektoru útoku

Sondy

- Výzkum&vývoj navazujících technologií (400 Gb/s)
- Zlepšení schopností měřících bodů (např. využití IDS, výpočet statistik)
- Analýza - klasifikace a detekce v šifrovaném provozu
  měřící body budou primárním zdrojem dat

Více podrobností v bloku o bezpečnosti ve čtvrtek...

cesnet 25

Děkujeme za pozornost