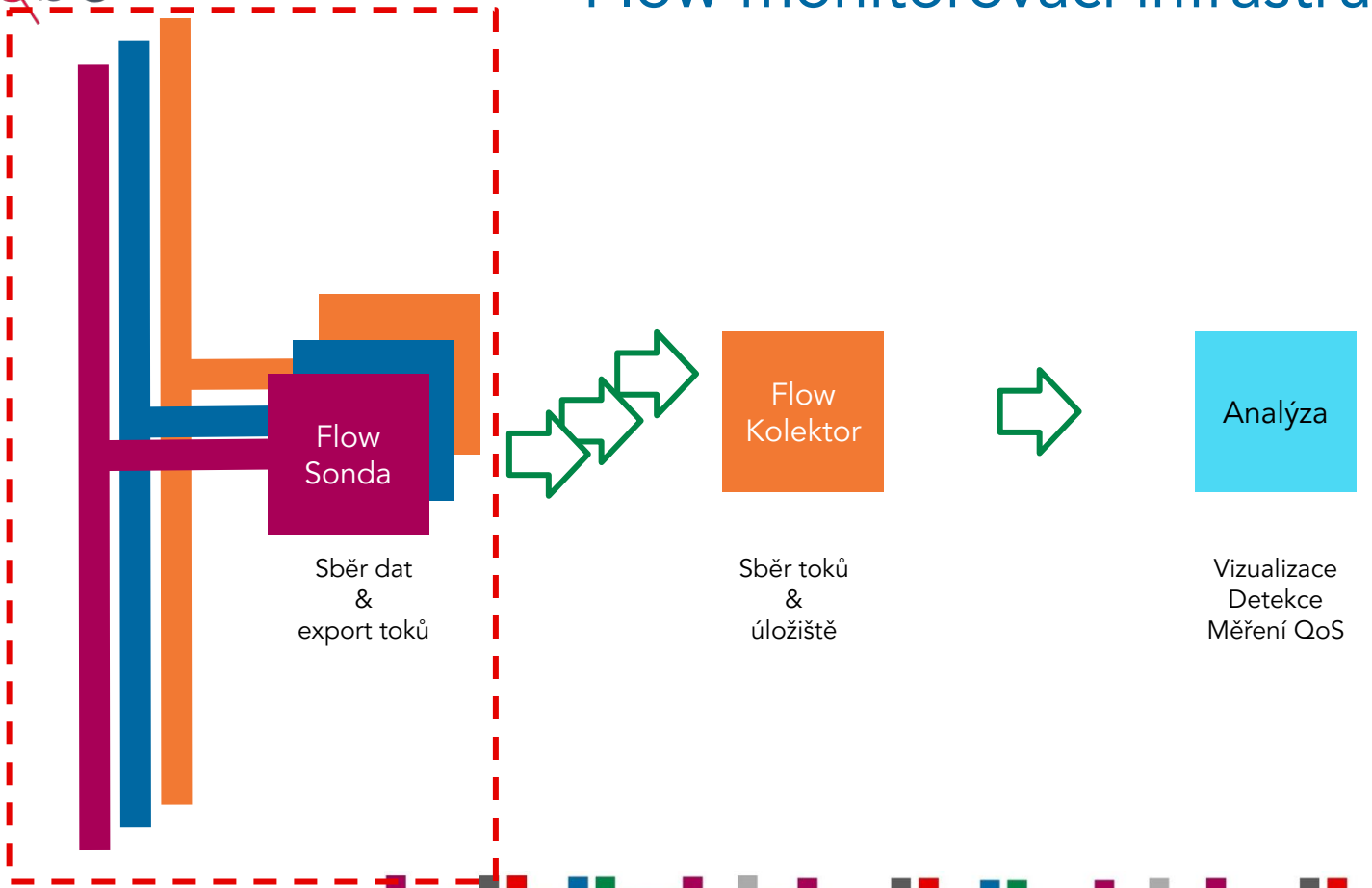
cesnet

Novinky a plány v monitorování sítí pomocí ipfixprobe

Karel Hynek | Traffic Analysis, CESNET

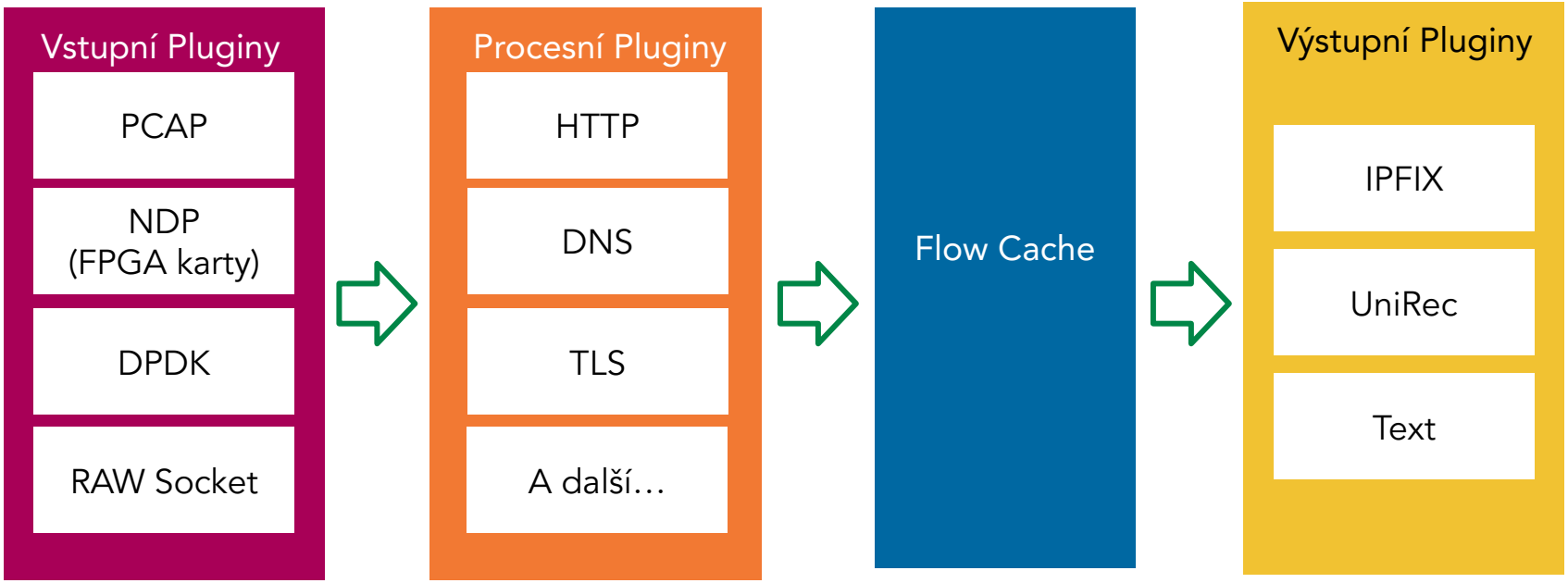
ipfixprobe

Flow monitorovací infrastruktura



ipfixprobe

Modulární exportér síťových toků



ipfixprobe

Základní a rozšířená data

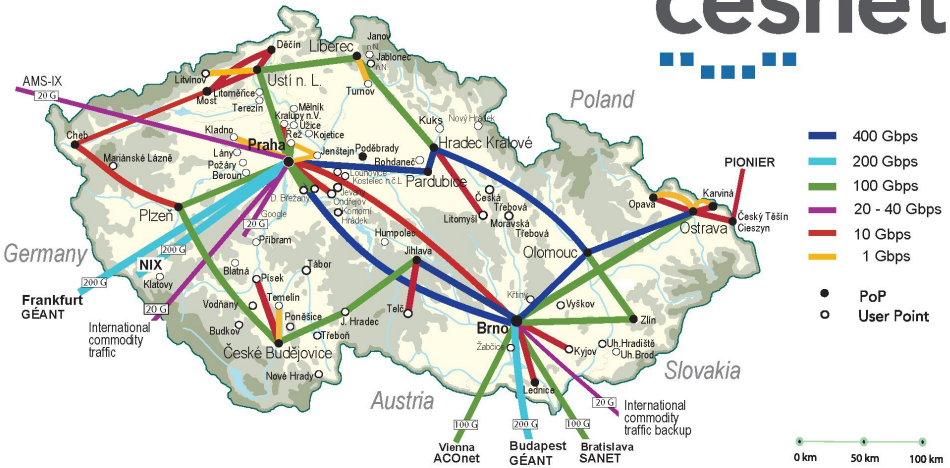
- Jednosměrné flow / Obousměrné flow
- Klasické informace z NetFlowV5
  - IP adresy, MAC adresy, Porty, počet bajtů, počet paketů (v jednotlivých směrech v případě biflow)
- Podpora AI
  - pstats - Sekvence Paketových délek a časů pro prvních 30 paketů
  - phists - Histogramy paketových délek a časů
- Podpora parsování protokolů
  - HTTP, TLS, DNS, WG, DNS, RTSP, MQTT, SMTP…

Dostupnost

- Dokumentace na https://cesnet.github.io/ipfixprobe/
- Zdrojové C++ kódy jsou dostupné na GitHub
- Balíky pro EPEL8, EPEL9
  - https://copr.fedorainfracloud.org/coprs/g/CESNET/NEMEA/
- Dostupné ve standardních repozitářích TurrisOS, Alpine Linux…
- Podpora při produkčním nasazení ipfixprobe - Nadstandardní služba v rámci CESNET

Nasazení v CESNET

- Monitoring perimetru sítě CESNET3
  - Hlavních 8 peeringových linek s propustností >100G
- Komoditní servery DELL
  - Obvykle 2U R740, 2x CPU, FPGA SmartNICs s vlastním firmware
- Servery monitorují obvykle více linek
- Bezztrátová propustnost 175 Gbps



Nasazení ve světě

- Dresden University of Technology
  - Monitorování 100G uplinku

- ROWANet - páteřní síť kraje Vysočina
  - Monitorování peeringu

- Pilotní testování v seznam.cz

- Klíčová technologie pro realizaci bezpečnostních MO/MV projektů

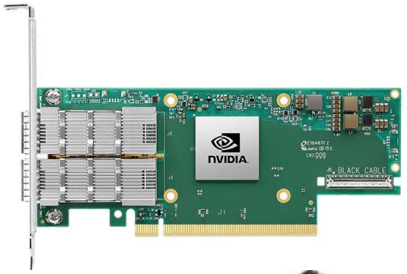
ipfixprobe

Novinky a plány

DPDK vstupní plugin

- Možnost spuštění ipfixprobe jako sekundární DPDK aplikace
- Podpora běžných SmartNIC. Odzkoušeno na:
  - Nvidia Mellanox ConnectX-6 (2x100G)
  - Broadcom N1400GD (1x400G)
- Úprava bufferování — snížení ztrátovosti při saturaci linky
  - Nové schéma vylepšuje propustnost cca 1000x

DPDK
DATA PLANE DEVELOPMENT KIT



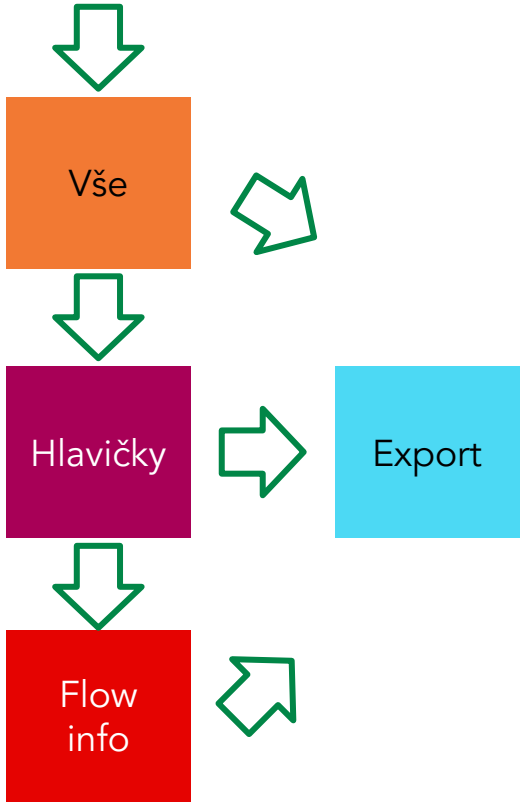
ipfixprobe

Zpracování protokolu QUIC

- QUIC je použit pro HTTP/3 — Majoritně jej používá Google
- Obfuskace navazování QUIC spojení pomocí AES-128-GCM
  - ipfixprobe musí tyto pakety dešifrovat aby je mohl naparsovat
- Extrakce nových informací
  - Connection IDs
  - Indikace použití 0-RTT
  - …
- Vylepšený packet processing — zvládáme procesovat QUIC i na našem 40G peeringu s Google

Monitorování 400G

- Problém jak dostat data z karty do CPU
  - PCIEx16-GEN5 přenese ~500 Gbps
  - PCIEx16-GEN6 přenese ~900 Gbps
- Offload tvorby flow záznamů v NIC FPGA firmware
- Offload pro heavy toky
  - Více jak 70 % dat je přeneseno v 10 % toků
- Interně testujeme



Vytvořeno v rámci projektu VJ02010024, IMPAKT, MVČR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Konfigurátor PANDDA

- Zjednodušení tvorby a orchestrace monitorovací
  - ipfixprobe je klíčovou částí

cesnet

dokumentace

Děkuji za pozornost!

Pro podporu s ipfixprobe mě kontaktujte na: hynekkar@cesnet.cz