Softwarově definované monitorování 100 Gb sítí

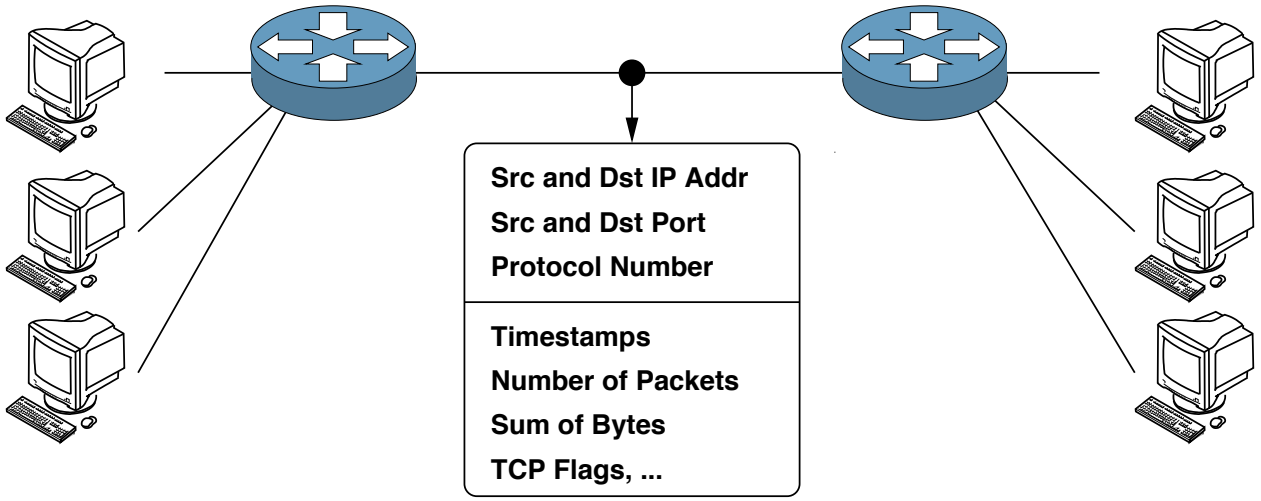
Viktor Puš, CESNET

23. 5. 2014

Konference Internet a technologie 14

Motivace

- Požadavky na monitorování infrastruktury
  - Ochrana uživatelů a investic
  - Detekce anomálií a bezpečnostních hrozeb
- NetFlow monitorování



Rozvoj monitorování

- Posun monitoringu na aplikační vrstvu (L7)
  - Protokoly HTTP, DNS, SIP
  - Proč? Heartbleed a další
- 100 Gb/s technologie začíná být dostupná
  - 150 Mpaket/s (6,7 ns/paket)

➔ **L7 Monitorování na 100 Gb/s**

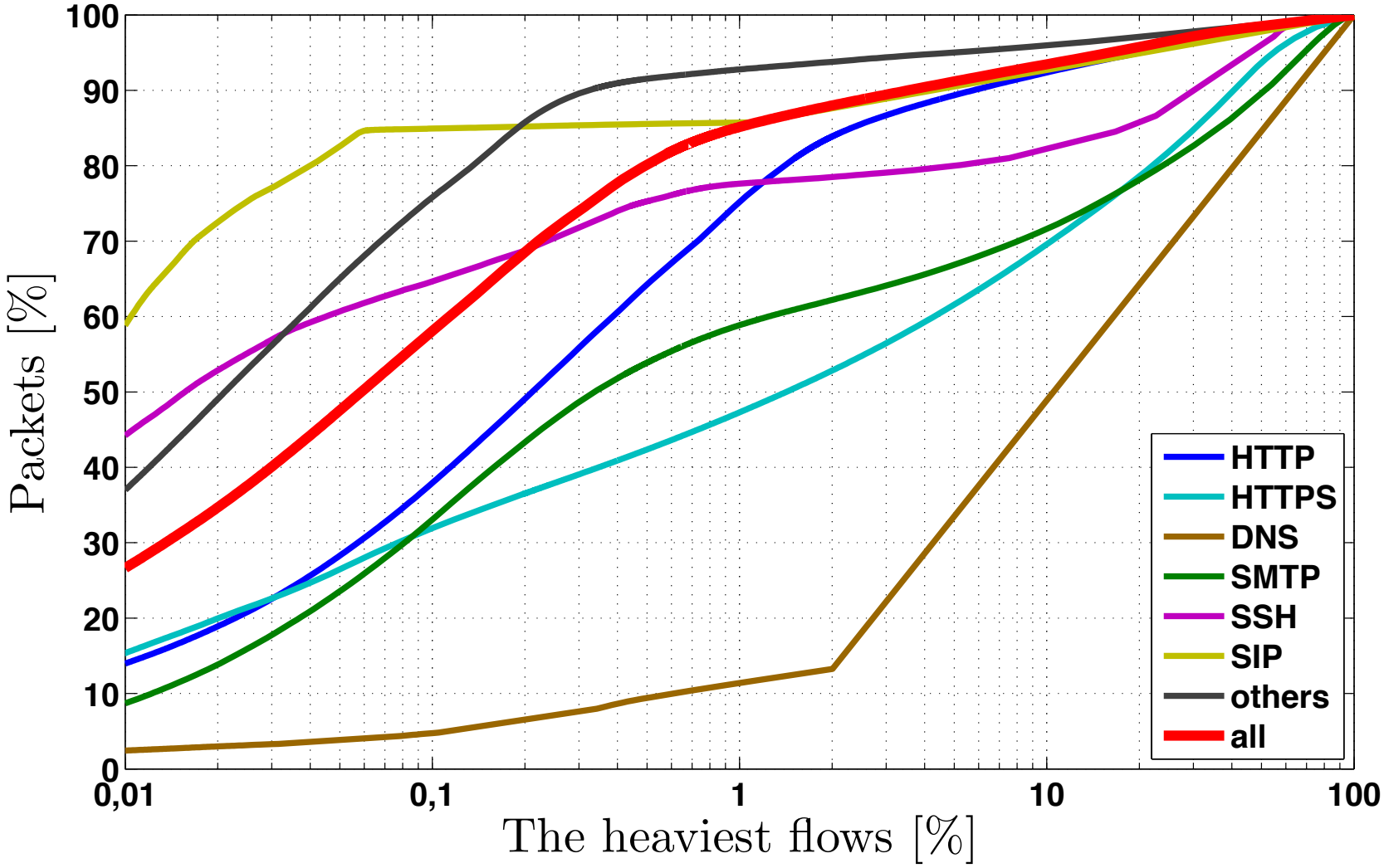
Jak monitorovat 100 Gb/s?

- Limit CPU je okolo 20 Mpaket/s/jádro při obyčejném NetFlow měření
  - Pouze základní statistiky do úrovně TCP/UDP
  - Zpracování L7 je výpočetně mnohem náročnější
- Kompletní implementace monitorování v hardware
  - Zpracování stále L7 předmětem výzkumu
  - Malá flexibilita
- Je možné najít kompromisní řešení?

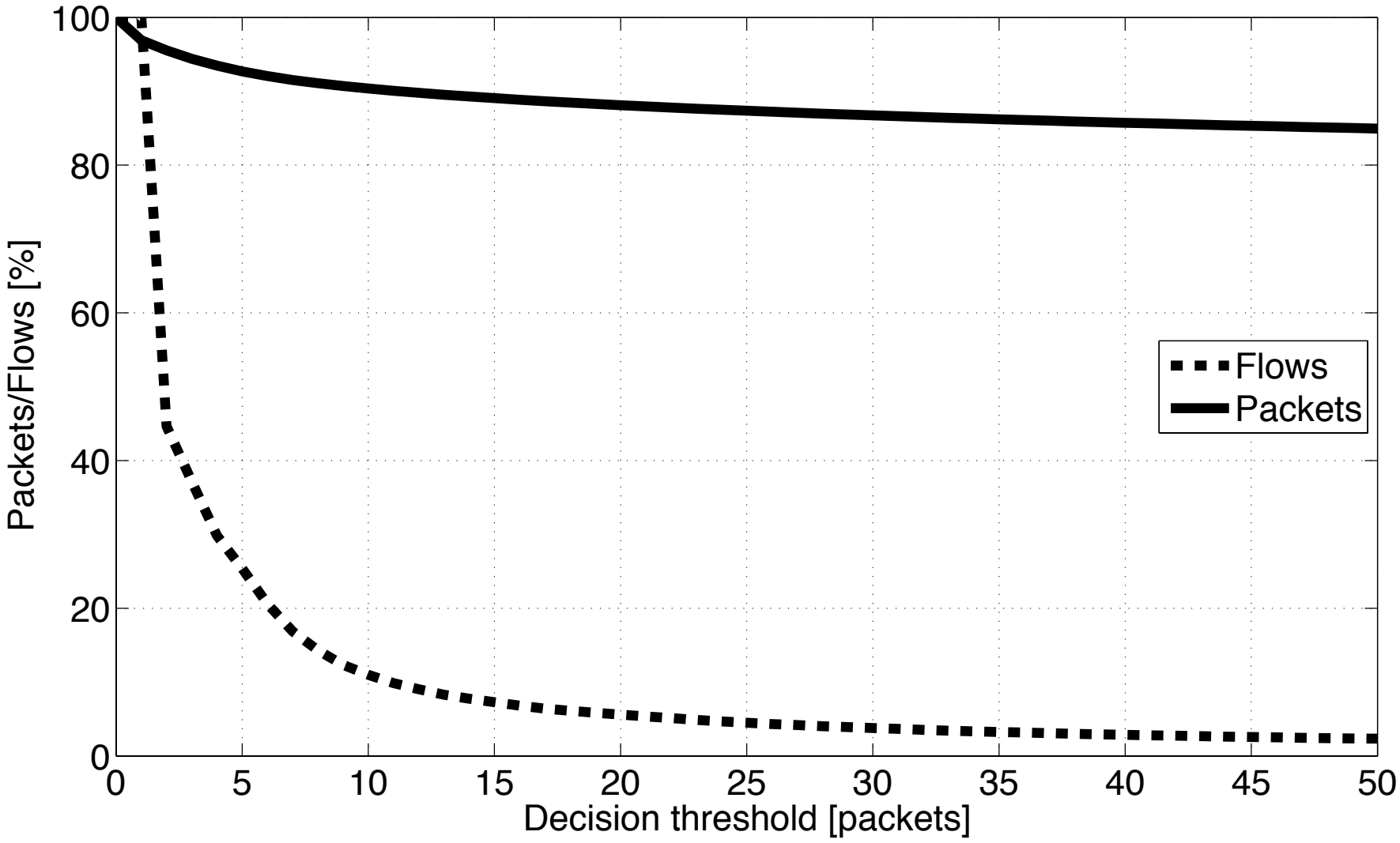
Koncept SDM - teze

- Síťový provoz má heavy-tail rozložení
  - Velký podíl provozu tvoří malé množství velmi velkých toků
  - Většina provozu je nezajímavá (download, streaming, ...) – stačí NetFlow měření
- **HW (NetFlow) zpracováním malého množství toků výrazně odlehčíme CPU (L7)**
- Jak detekovat těžké toky?
  - Jak přesně a rychle je to potřeba dělat?
- Jaký bude vliv na výkonnost a flexibilitu?

Heavy tail – distribuční fce



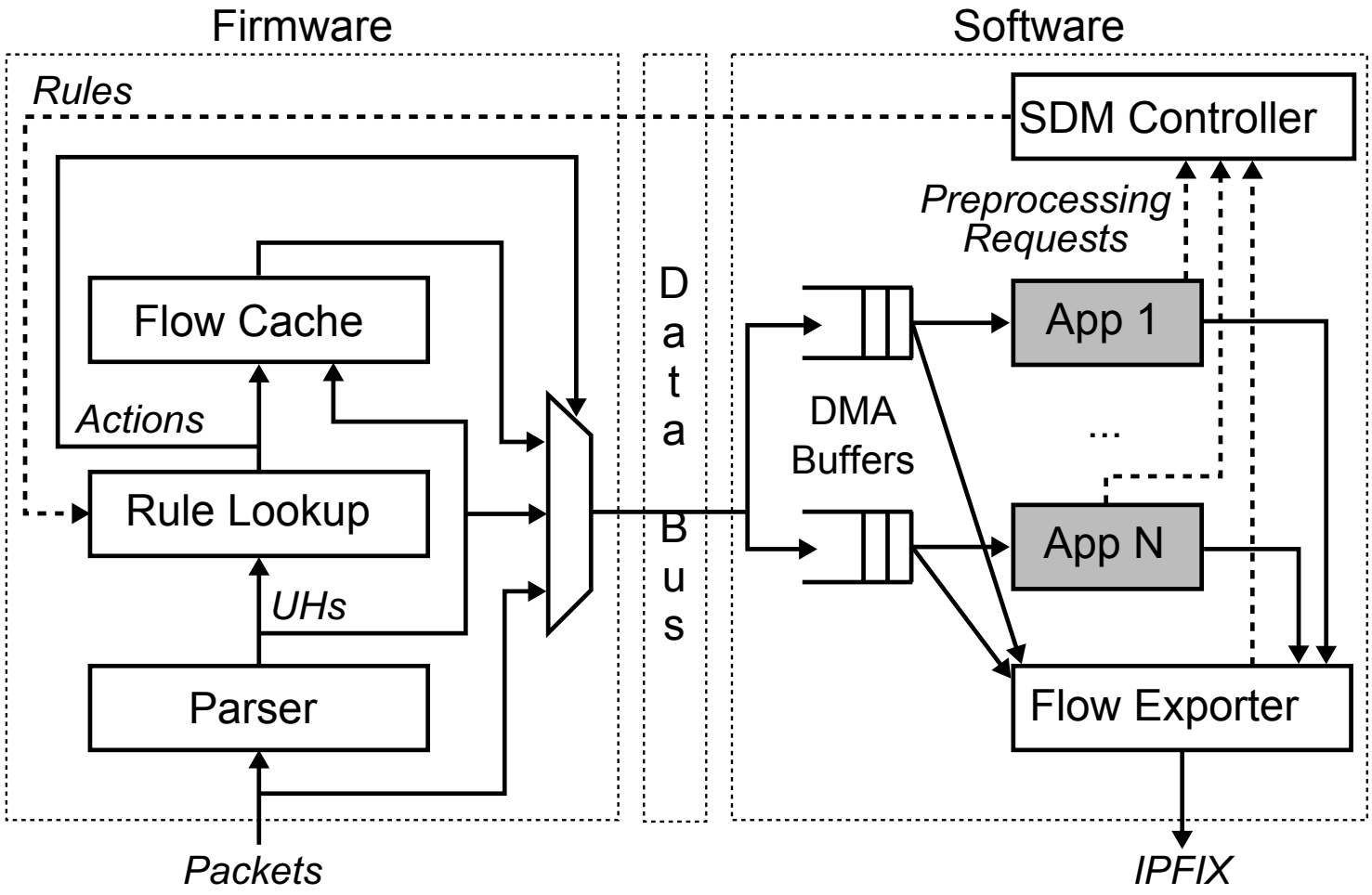
Efekt


100
80
60
40
20
0
Packets/Flows [%]
0
5
10
15
20
25
30
35
40
45
50
Decision threshold [packets]
Flows
Packets

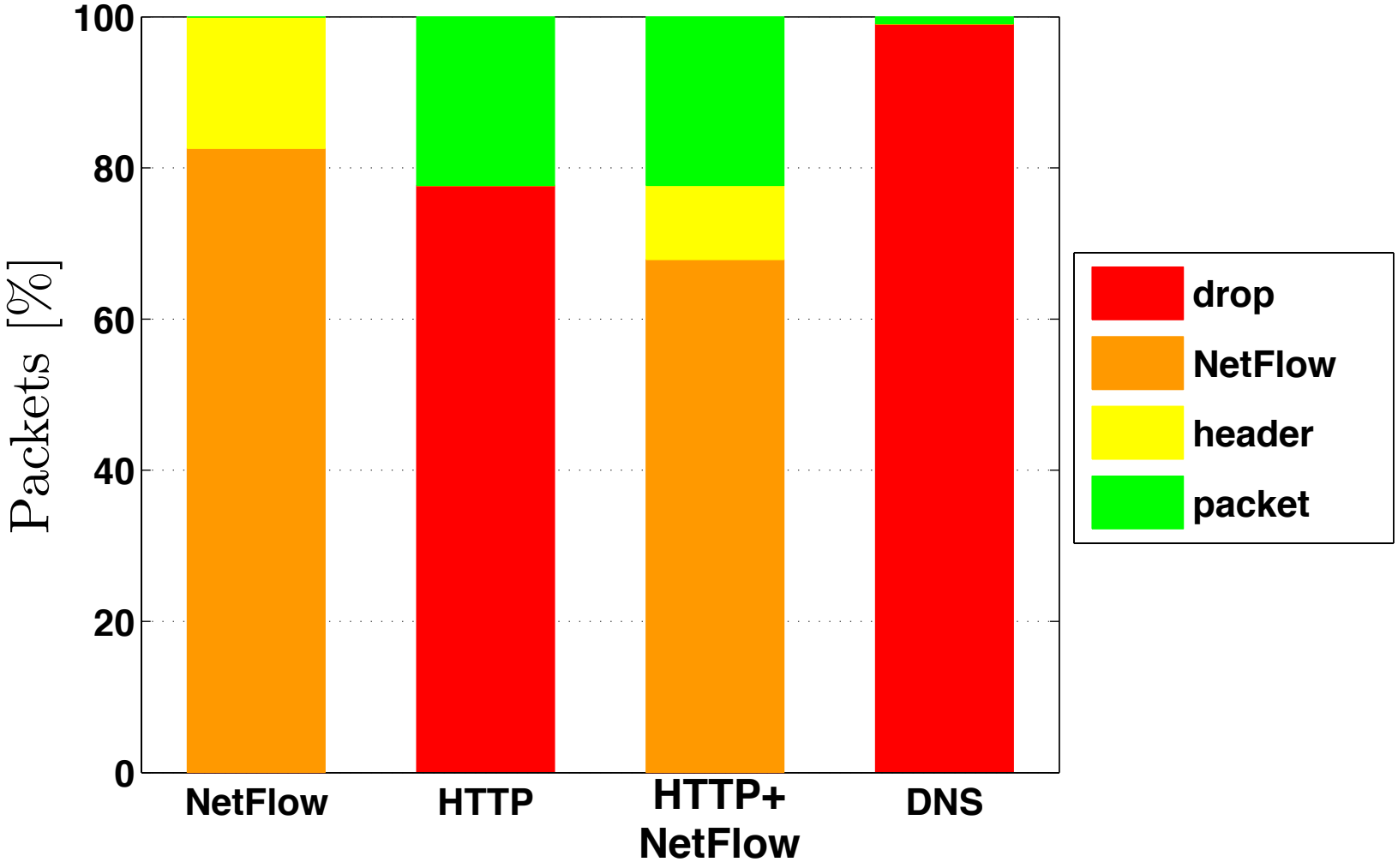
Koncept SDM - návrh

- Nové “neznámé” toky předány do CPU
- **Software rozhoduje** o způsobu zpracování každého toku
  - Softwarové zpracování zajímavého/podezřelého provozu
  - Hardwarové zpracování pouze velkých a “nezajímavých” toků
    - Které ale tvoří většinu provozu!
- Systém SW pluginů (psaných v C)
  - Změna chování bez změny nebo detailní znalosti HW

SDM – schéma


Firmware
Software
Rules
SDM Controller
Preprocessing Requests
Flow Cache
Actions
Rule Lookup
UHs
Parser
Packets
Data Bus
DMA Buffers
App 1
...
App N
Flow Exporter
IPFIX

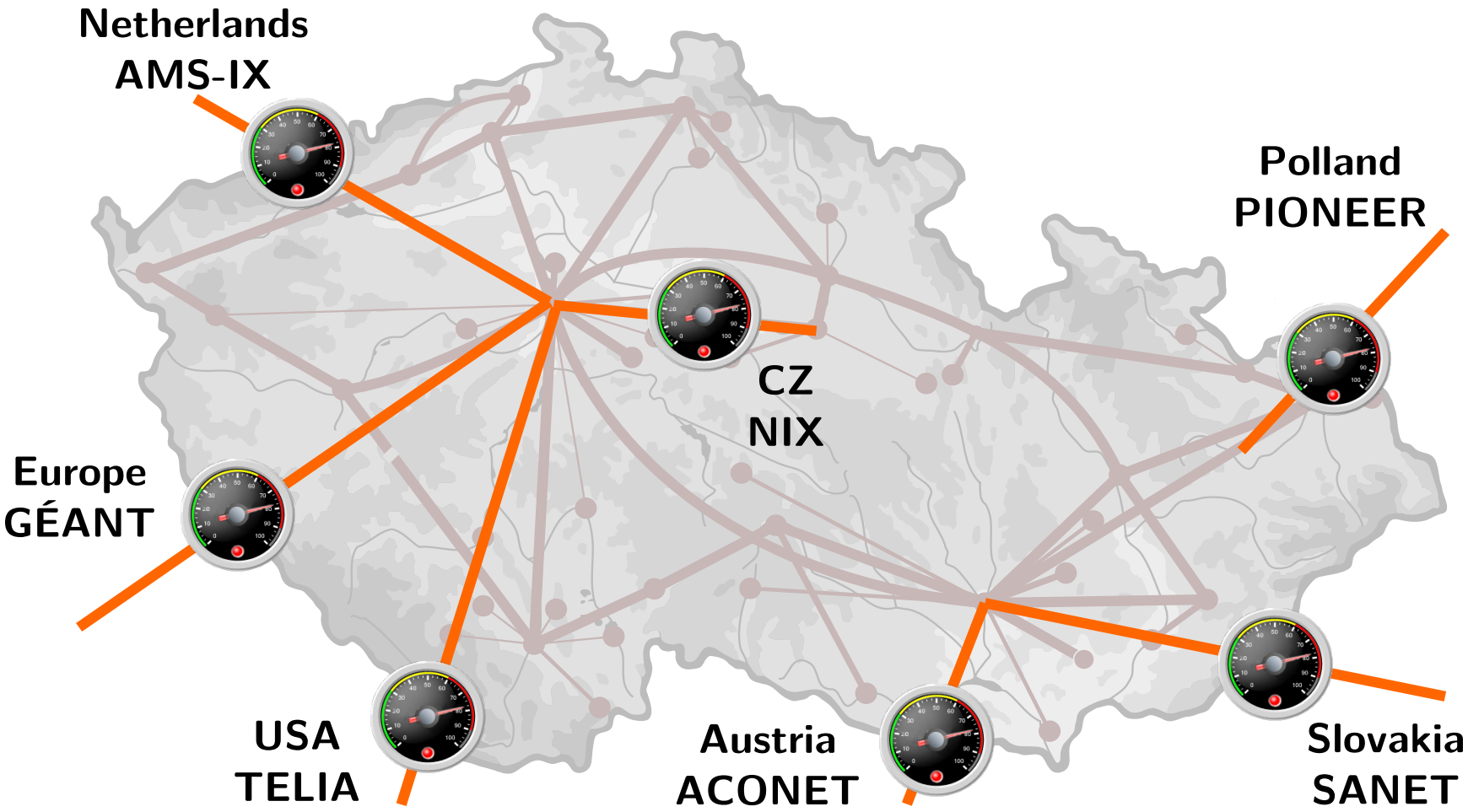
Use case: HTTP



Náš hardware

- Karty s FPGA Virtex-7
- 100G:
  - CFP2 optický modul
    - 100GBASE SR10, LR4, 10x 10GBASE
  - PCI-Express gen3 x16
    - Až 128 Gb/s
  - 3x QDR
- 80G:
  - 2x QSFP+ optický modul
    - 2x 40GBASE nebo 8x 10GBASE
  - PCI-Express gen3 x8
  - 1x QDR

Měření perimetru sítě



Závěr

- Nástroj pro monitorování na 100 Gb/S
  - **Flexibilní** prostřednictvím SW pluginů
  - **Výkonný** s pomocí HW akcelerátoru
- Firmware implementován pro kartu 8x10Gb
  - Propustnost **cílově 100 Gb/s**
- V plánu
  - Nasazení do monitorovací infrastruktury
  - Rozšíření funkce firmware o prvky L7 analýzy

Děkuji za pozornost