Systém pro monitorování síťových protokolů

Autor: Ing. Roman Selecký, selecky@fit.vutbr.cz
Vedoucí: Ing. Jan Kořenek, Ph.D., korenek@fit.vutbr.cz

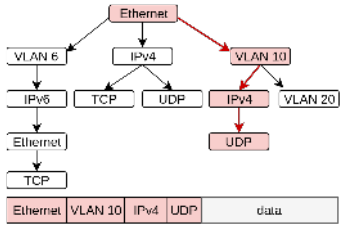
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Motivácia

1. Diagnostika sietí a detekcia nežiadúcej prevádzky
2. Monitorovanie sieťových tokov a štruktúry protokolov
3. Záchyt na základe zapúzdrenia protokolov

Štruktúra protokolov

- Pod pojmom štruktúra protokov, rozumieme poradie, v ktorom sú hlavičky protokolov v rámci paketu zapúzdrené.
- Získané sekvencie identifikátorov hlavičiek, tzv. **signatúry**, môžeme vizualivovať vo forme **stromu protokolov**.
- Signatúra, predstavuje cestu v strome smerom od koreňa k listovým uzlom.
- Strom protokolov môže obsahovať viacero uzlov označujúcich ten istý protokol.



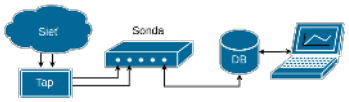
Obrázek 1: Signatúra paketu zobrazená v strome protokolov

- Každý sieťový tok môžeme asociovať s uzlom stromu protokolov, ktorý odpovedá poslednému protokolu signatúry.
- Na základe toho je možné pre každý uzol stromu protokolov počítať volumetrické informácie

Návrh systému

Monitorovací systém je založený na monitorovaní tokov, preto jeho spôsob nasadenia odpovedá schémam protokolov NetFlow a **IPFIX**.

- Monitorovacie zariadenie, **sonda**, je do siete pripojené prostredníctvom zariadenia Tap. Toto zariadenie preposiela celú sieťovú prevádzku do sondy, ktorá vykonáva samotnú monitorovaciu činnosť.
- Získané informácie odosiela na úložisko dát, tzv. **kolektor**, ktorý je na obrázku reprezentovaný symbolom databázy.
- K perzistentne uloženým dátam je možné pristupovať z počítača, ktorý slúži k ich vizualizácií prostredníctvom **užívateľského rozhrania**.

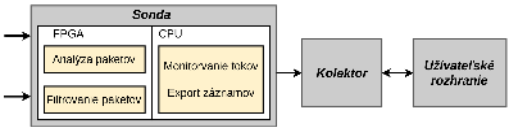


Obrázek 2: Schéma zapojenia systému

Dekompozícia systému

Monitorovací systém sa skladá z dvoch výpočtových častí:

- **Sonda** zodpovedá za monitorovanie tokov a filtrovanie paketov. Jednotlivé úlohy sú mapované na:
  - **FPGA** čip je určený na akceleráciu časovo kritických operácií vykonávaných s príchodom každého paketu, teda: analýzy paketov, extrakcie položiek z hlavičiek protokolov a filtovanie paketov. Flexibilita je dosiahnutá využitím generátoru z vysokoúrovňového popisu protokolov v **jazyku P4** do jazyka VHDL.
  - **Procesor** je vhodný na vykonávanie komplexnejších a pamäťovo náročných úloh, medzi ktoré patrí monitorovanie a export tokov.
- **Kolektor** perzistentne ukladá dáta vygenerované monitorovacím procesom na sonde. Z dôvodu univerzálnosti je použitý štandardizovaný spôsob prenášania a ukladania informácii o sieťovej prevádzke - protokol IPFIX, ktorý je rozšírený o aplikačne špecifické informácie, napr. signatúru.

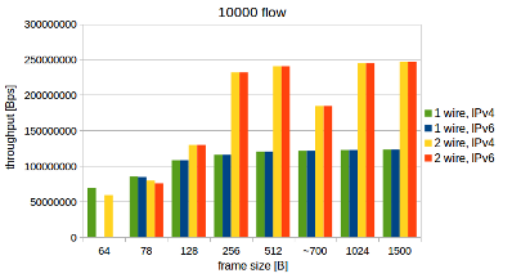


Obrázek 3: Dekompozícia úloh medzi výpočtové časti systému

Obrázek 4: Fotografia cieľovej platformy

Záver

- Implementovaná hardvérová a softvérová časť, GUI, zmeny v IPFIX kolektore
- Vytvorené testovacie prostredia
  - Funkčné verifikácie - pokrytie kódu 96%
  - Prostredie automatizovaných testov
- Zmerané parametre systému
  - Nízka spotreba zdrojov v FPGA - 8% ALM, 1% BlockMem
  - Vysoká priepustnosť



Obrázek 5: Priepustnosť systému meraná na sonde s dvoma 1Gbps vstupnými rozhraniami