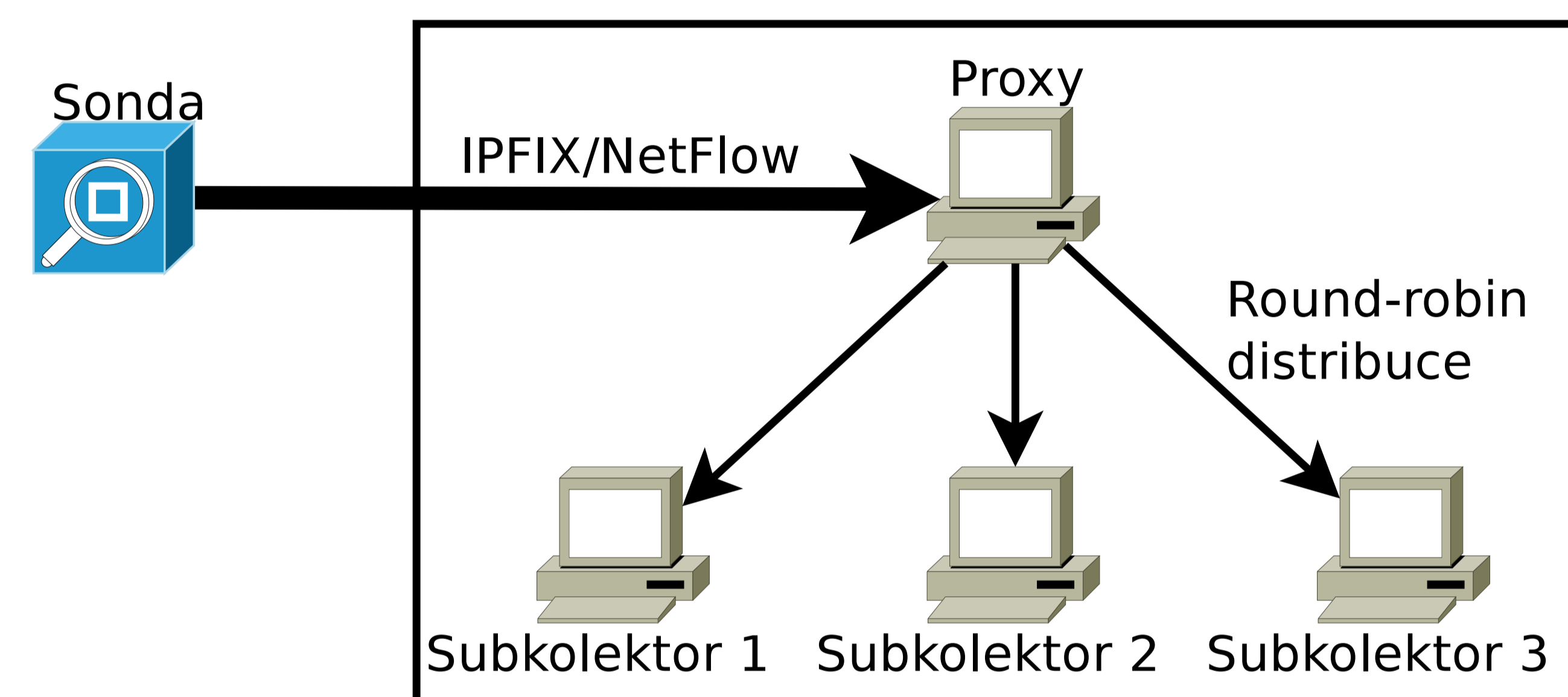


Motivace

- ▶ Kolektor hraje významnou roli při analýze záznamů o tocích a při dohledávání incidentů a kybernetických útoků.
- ▶ Roste ale jak počet záznamů tak počet dotazů nad daty.
- ▶ Díky tomu se kolektor, jakožto centrální bod monitorovacího řetězce, snadno může stát úzkým hrdlem.
- ▶ Centralizované řešení naráží na své výkonnostní limity v prostředí rozsáhlých a vysokorychlostních sítí.
- ▶ Implementace distribuovaného řešení je teprve v počátcích a je potřeba hledat řešení, která dokážou plně využít potenciál distribuovaného systému.

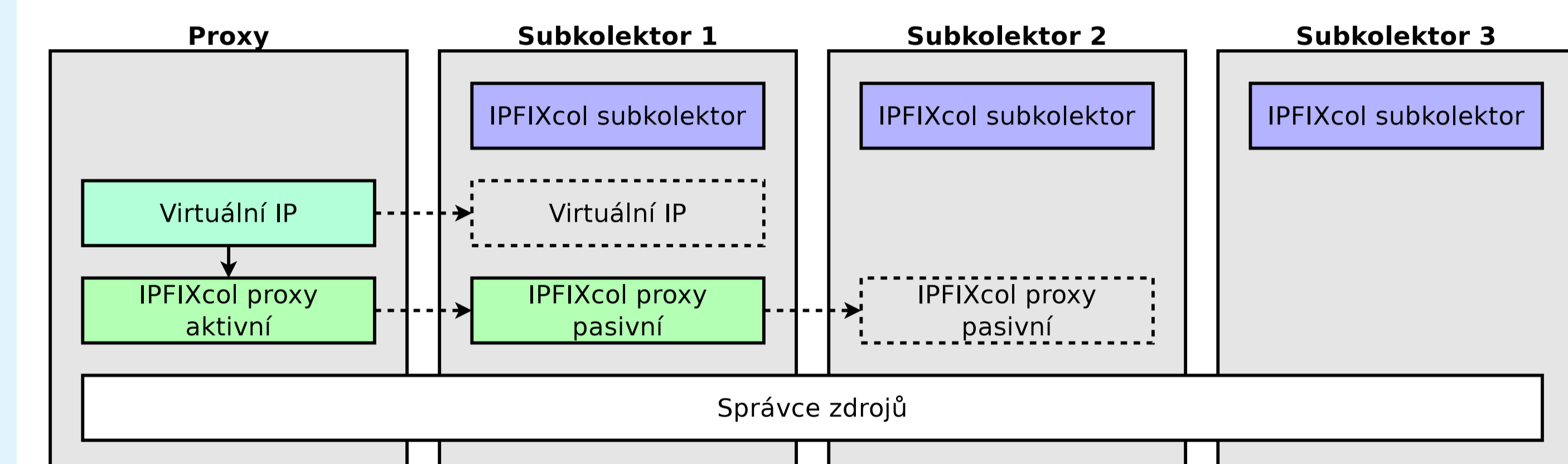
Architektura distribuovaného kolektoru

- ▶ Proxy:
 - ▶ vstupní bod pro data ze sond a pro uživatele,
 - ▶ vyvažovač zátěže,
 - ▶ neuchovává data.
- ▶ Subkolektor:
 - ▶ pro okolní svět neviditelný,
 - ▶ uchovává data.



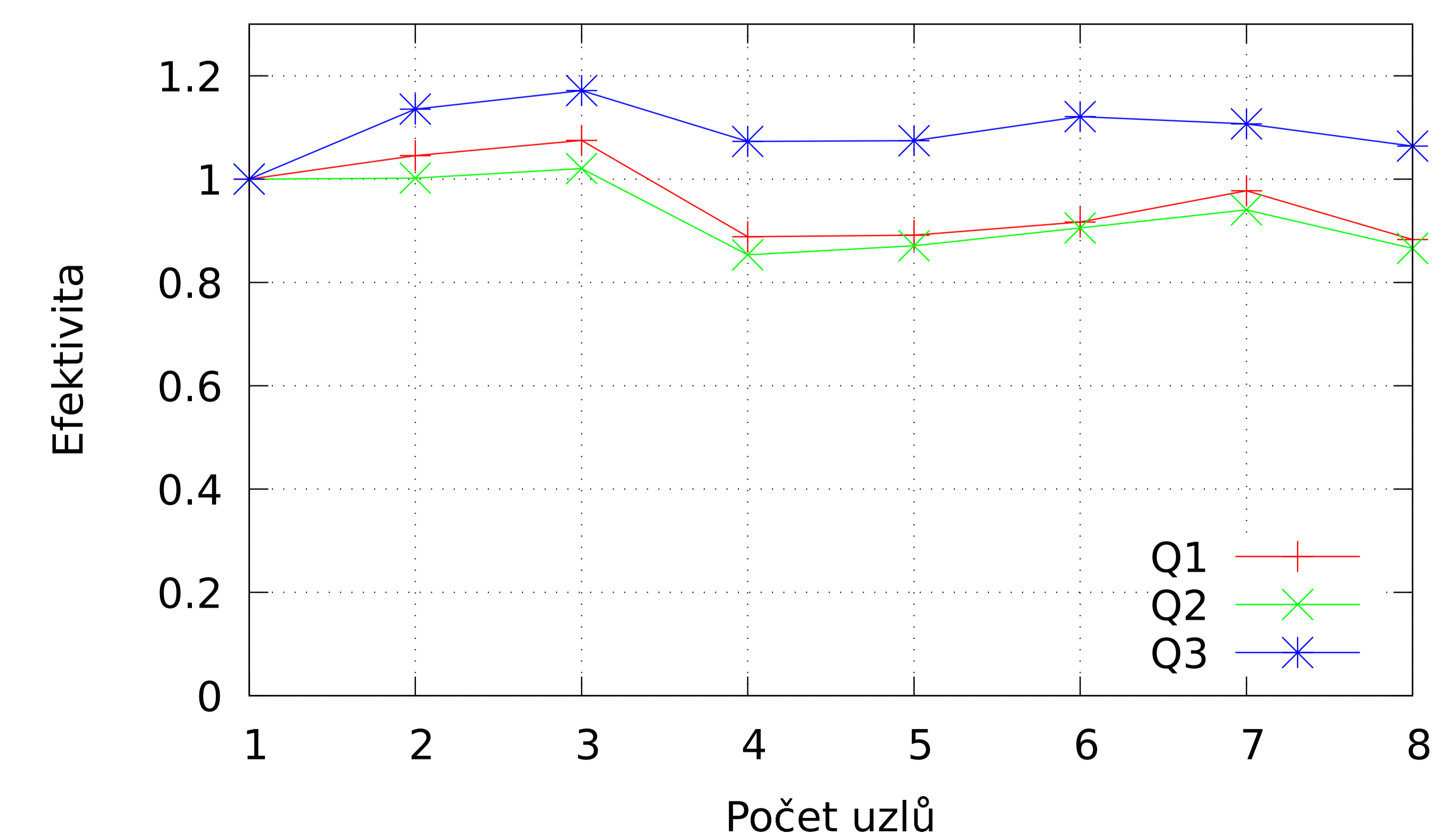
Vysoká dostupnost a odolnost proti poruchám

- ▶ Automatický failover při výpadku uzlu nebo služby zajišťuje správce zdrojů.
- ▶ Datová redundance zajištěna vzájemnou kruhovou replikací dat mezi subkolektory.



Výsledky a zhodnocení

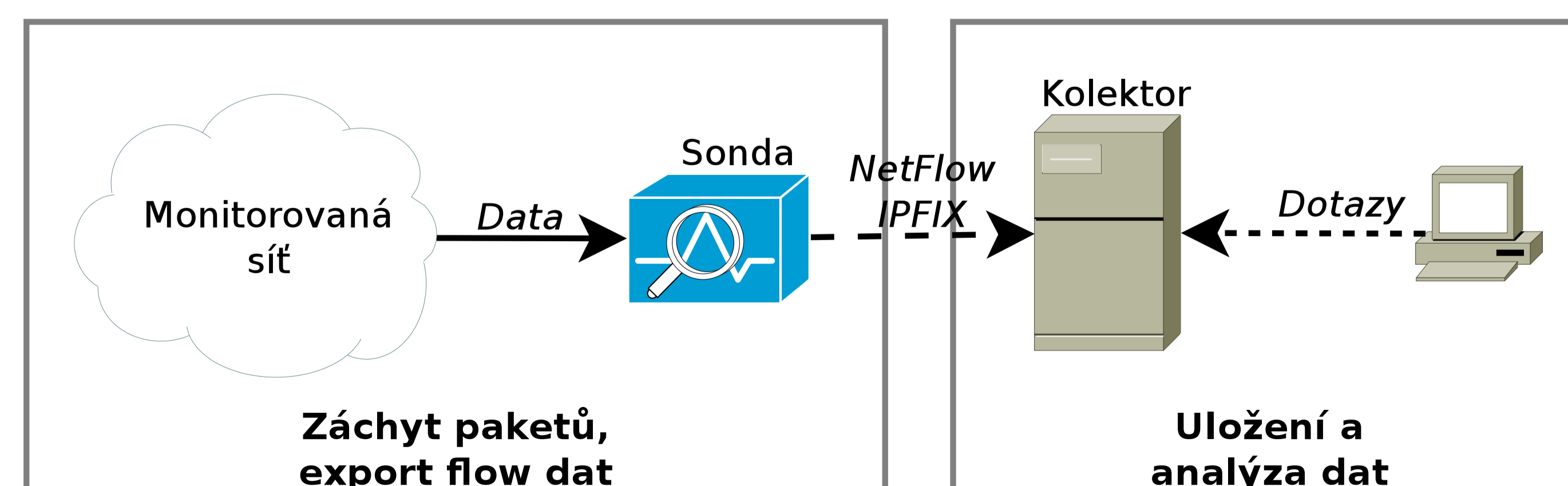
- ▶ Architektura bez jediného bodu selhání.
- ▶ Doba trvání detekce poruchy softwaru nebo hardwaru v jednotkách sekund.
- ▶ Lineární růst výkonu dotazovacího systému s rostoucím počtem uzlů.



Monitorování síťových toků

Jde o oblíbený způsob monitorování síťového provozu, který se skládá z několika fází:

1. záchyt a předzpracování paketů,
2. měření a export toků,
3. sběr a uložení dat,
4. analýza dat.



Dotazovací systém

- ▶ Distribuovaná master/slave architektura.
- ▶ Datová dekompozice problému.
- ▶ Žádný přesun surových dat mezi uzly.

