Turris:Sentinel

Sběr dat a dynamický firewall znovu a lépe

Martin Prudek • martin.prudek@nic.cz • 14. 11. 2019

CZ.NIC | SPRÁVCE DOMÉNY CZ

Osnova

- Historie, starý systém
- Sentinel – nový systém
- Stav vývoje a nasazení

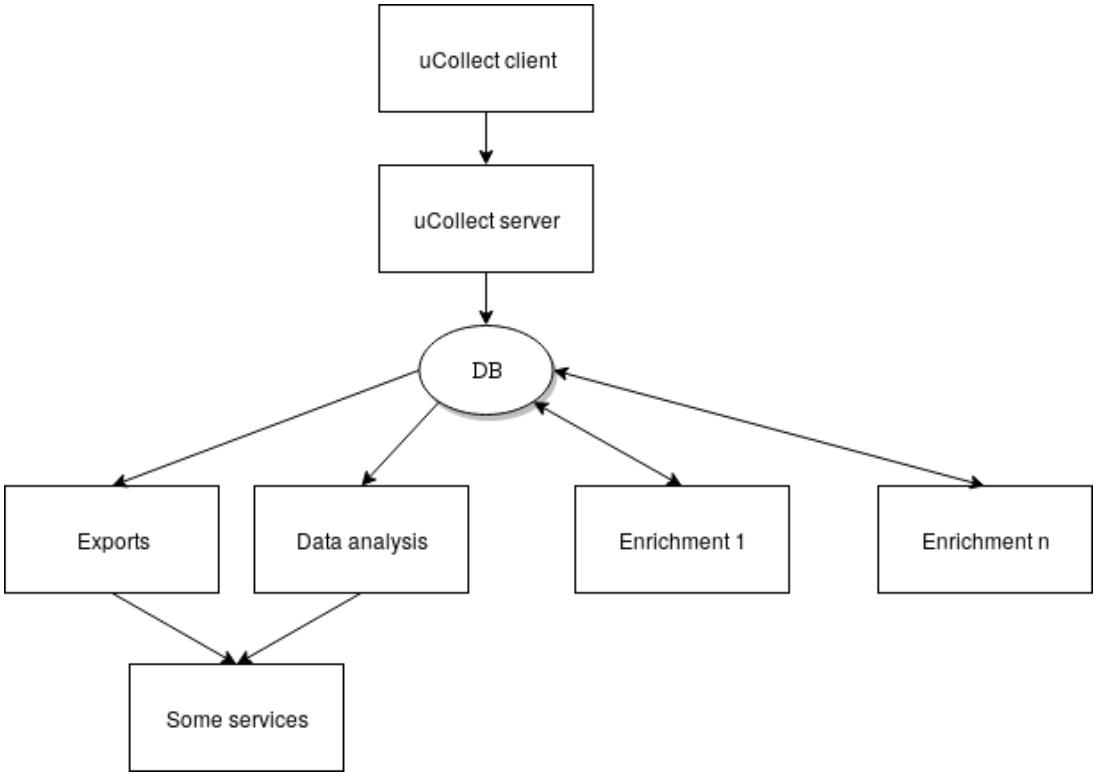
Historie – Turris a sběr dat

- Je s námi již od začátku
  - Turris je původně výzkumný projekt
  - Modré routery (Turris 1.0, Turris 1.1) rozdávané proti nájemní smlouvě
  - Sběr dat integrální součástí projektu
- Výstupy
  - Greylist
  - Dynamický firewall
  - Statistiky

uCollect – starý systém

- Řešení psané
  - Na daný počet zařízení
  - S danými výhledy a plány
- Nevyužívané funkce omezují škálovatelnost
- Klient-server řešení
- Data ve velmi stresované databázi

uCollect – starý systém



uCollect – starý systém

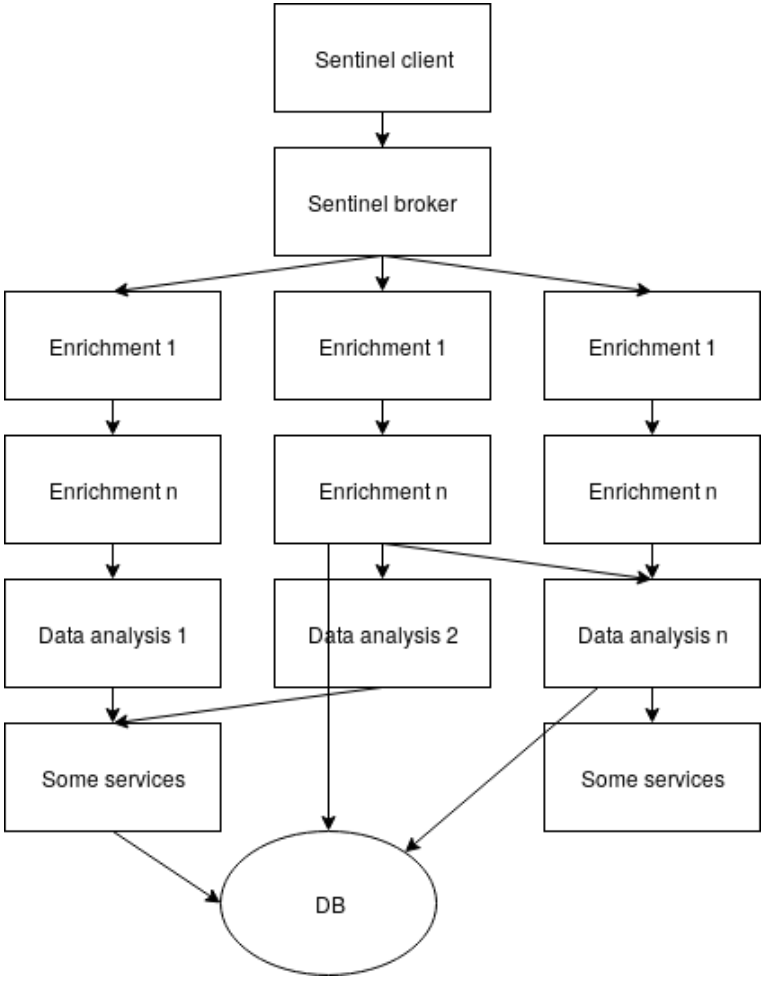
- 2 úzká hrdla
  - Klientský protokol
    - Zbytečně složitý
    - Vázaný na jedno-instanční server
    - Nereálný přepis
  - Centrální DB
    - Za hranicí životnosti
    - Nelze přidávat další klienty ani analýzy

Sentinel – nový systém

- Základní motto: Připravit se na cokoliv
- Vše musí být škálovatelné dalším HW a dalšími instancemi
- Vše maximálně zjednodušit
  - Zahodit nepoužívané funkce původního návrhu
  - Proudové zpracování dat
  - Více hloupých krabiček lepší než jedna superchytrá

Sentinel – pipelining

- Pro každý zdroj dat jedna pipeline
- Činnosti
  - Příjem & validace dat
  - Obohacení
  - Analýzy
- Škálovatelnost
- Výstupy v reálném čase
- Databáze spíše pro účely archivace a statistik



Sentinel – technologie na serverové straně

- ZMQ
  - Brokerless
  - „TCP na steroidech“
  - Komunikační patterny – PUB/SUB, PUSH/PULL, REQ/REP
  - Load-balancing zdarma v rámci PUSH/PULL
  - Pro některé aplikace nevhodná
    - Pro uzly mimo vlastní infrastrukturu
    - Složitější zabezpečení
    - Nutná dodatečná funkcionalita v aplikačním protokolu

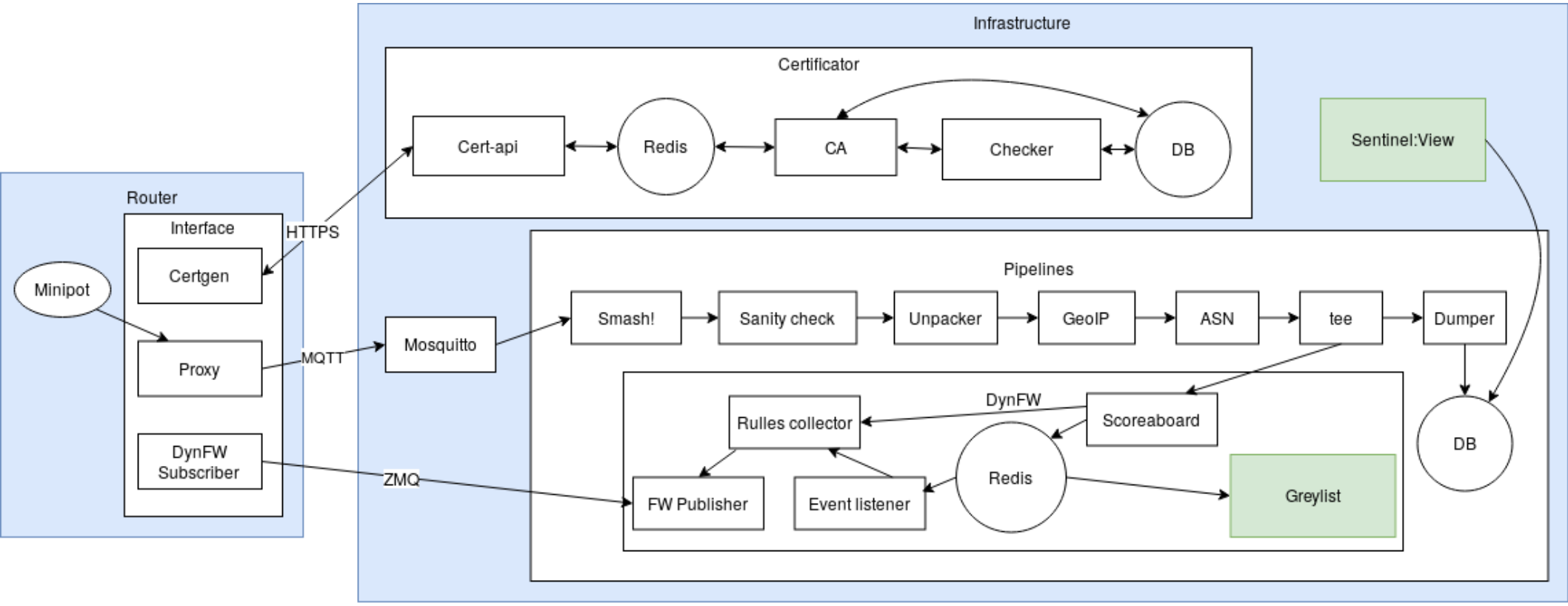
Sentinel – použité technologie

- MQTT pro ingress dat
  - Standardní řešení problému
  - Broker (Mosquitto)
  - Publish/Subscribe
  - Přihlášení pomocí klientského certifikátu, šifrování
  - Automatizovaná CA
  - Prozatím jeden uzel

Sentinel – analýzy

- DynFW
  - První a zatím jediná „analýza“
    - Sběr informací z mnho zdrojů
    - Přiřazování skóre útočníkům podle zavážnosti provinění
    - Po překročení limitu přidáme IP adresu do blacklistu
  - Vše realtime

Sentinel – architektura



Děkuji za pozornost

Martin Prudek • martin.prudek@nic.cz