Monitoring Turris Sentinel

Monitorujeme Sentinel pomocí Zabbixu

Lukáš Jelínek • lukas.jelinek@nic.cz • 22. 11. 2022

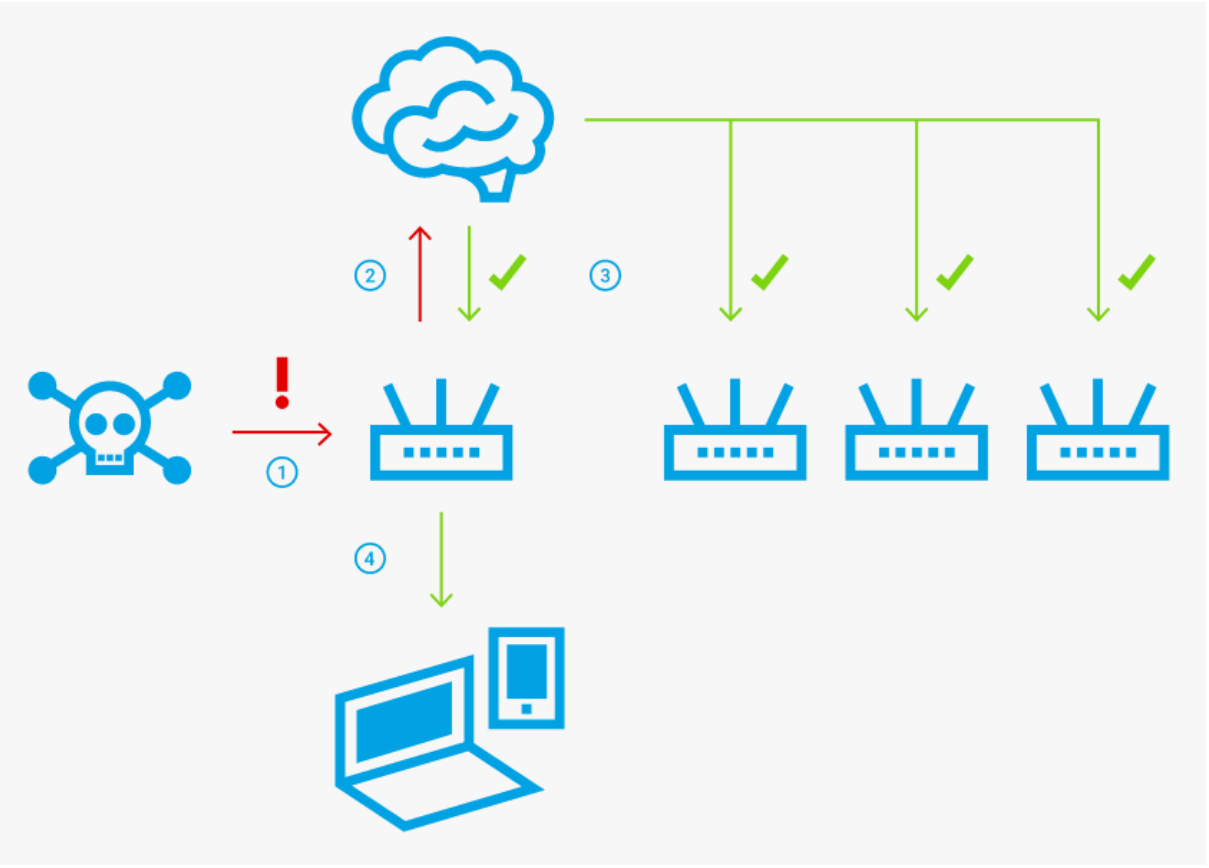
TURRIS

Co je Turris Sentinel

- **Bezpečnostní systém pro rychlou reakci na hrozby**
- Využívá data *dobrovolně* poskytovaná uživateli zařízení Turris
- Zdroje dat: minipoty, log firewallu, HaaS (v budoucnu další)
- Dynamický firewall – aktualizace v řádu sekund po detekci
- Přehled funkce – Sentinel View (https://view.sentinel.turris.cz)
- Zpracování dat – pipelines složené z jednotek („krabiček“)

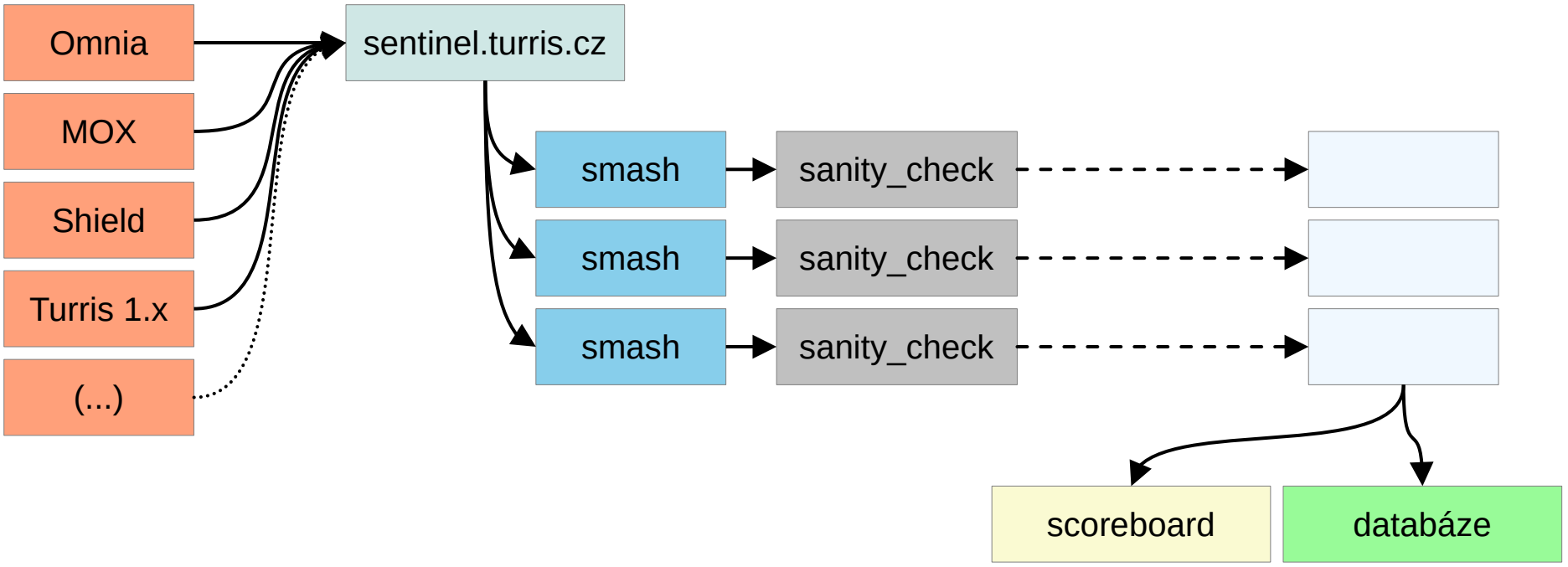
TURRIS

Jak vypadá Sentinel (celkově)



TURRIS

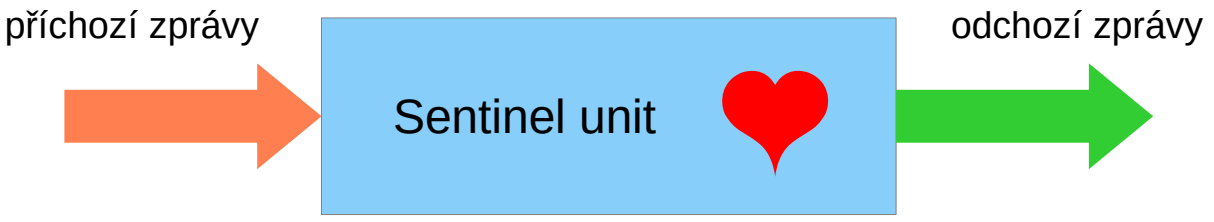
Jak vypadá Sentinel (uvnitř)



TURRIS

Co a proč potřebujeme monitorovat

- Mnoho komponent, každá se může porouchat
- Potřebujeme vědět, zda všechno „žije“
- Potřebujeme sledovat tok příchozích a odchozích zpráv



TURRIS

Jak nemonitorovat Sentinel

- **systemd / systemctl**
  - Detekuje nenaběhlé nebo spadlé jednotky, ale…
  - …to často nestačí…
  - Je potřeba vědět, že jednotka **opravdu žije**
  - Navíc nám nic neřekne o zprávách
  - (Ale stejně to používáme – pro všechny služby)

TURRIS

Monitoring pomocí Zabbixu

- Zabbix umožňuje příjem dat přes API
- Existuje referenční nástroj zabbix_sender
- Stačí sbírat údaje z jednotlivých jednotek a posílat je
- Každá jednotka zvlášť vs. centrální sběr vs. per server
- Uvnitř Sentinelu používáme IPv6-only síť
- Nechceme zbytečnou režii na sběr dat

TURRIS

Monitoring pomocí Zabbixu – realizace

- Každá jednotka má monitorovací výstup
- Máme jednotku čistě pro monitorovací účely
- Vlastní implementace komunikace se Zabbix API
- Co monitorujeme:
  - heartbeat (unixové časové razítko)
  - počet zpráv dovnitř
  - počet zpráv ven
- (V budoucnu můžeme přidat další parametry)

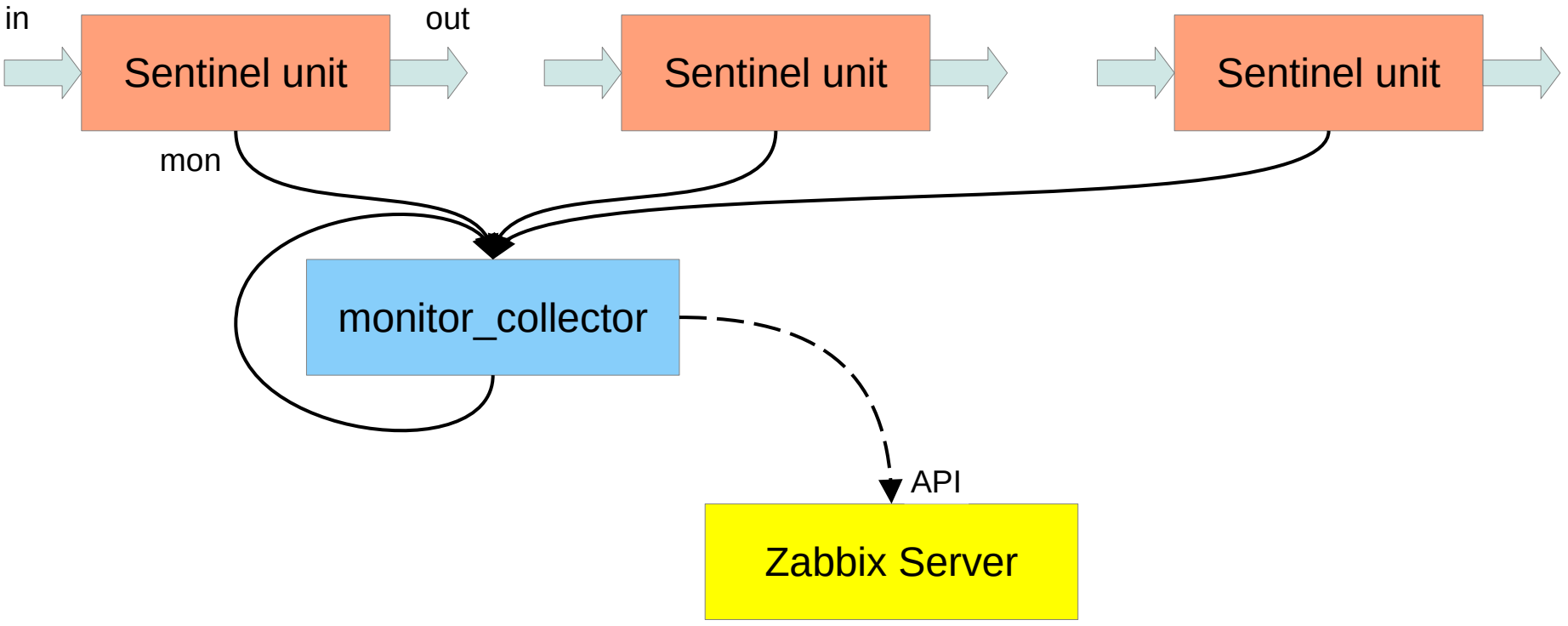
TURRIS

Monitoring pomocí Zabbixu – realizace

- Aktuálně jedna monitorovací jednotka na server
- V rámci Zabbixu řešeno pomocí discovery
  (změna sady jednotek bez ručních změn v Zabbixu)
- Triggery na heartbeat (detekce mrtvé jednotky)
- Lze přidat i triggery na zprávy (zatím nevyužíváme – složitější sémantika, více zájmových parametrů, velká variabilita)
- Zajímavé grafy: počty zpráv samostatně a „in vs. out“

TURRIS

Monitoring pomocí Zabbixu – realizace



TURRIS

Děkuji za pozornost!

Lukáš Jelínek • **lukas.jelinek@nic.cz**

TURRIS