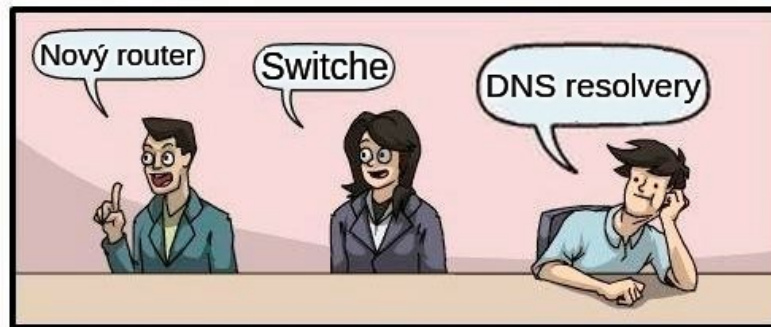


DNS pod kontrolou

Jak postavit moderní bezpečný resolver pro ISP

• 21. 01. 2026

Co jsou hlavní priority při správě sítě?



imgflip.com

Co se stane, když DNS resolver neodpovídá?

DNS Resolver Outage: Impact on Popular Services



Lost Revenue · Service Disruption · Support Overload

Jaké jsou požadavky na moderní DNS resolver

- Rychlost
- Spolehlivost
- Vysoká dostupnost
- Filtrování hrozeb
- Rate limiting / DoS prevention
- DNSSEC validace
- Soukromí

Rychlost & spolehlivost

- V první řadě je to o správné volbě SW & HW

Rychlost & spolehlivost

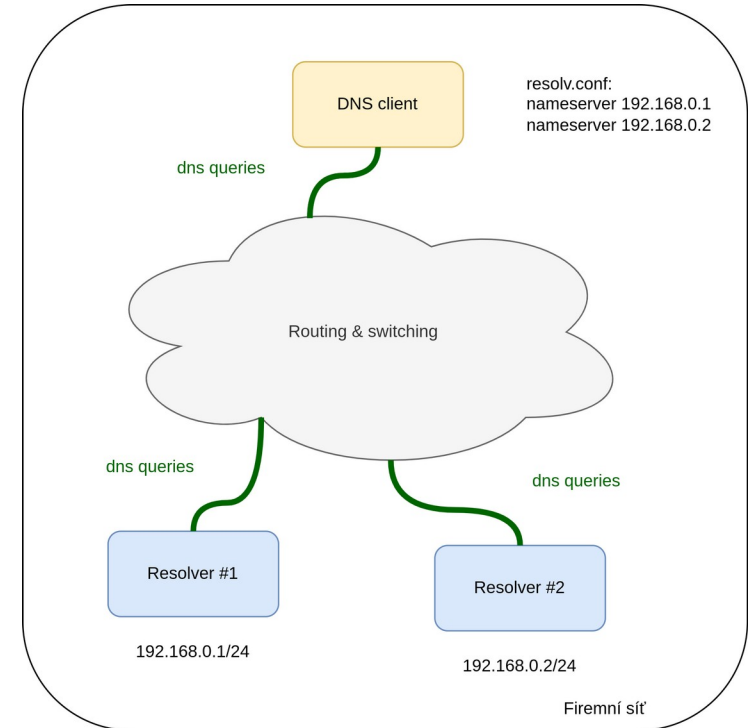
- HW dimenzovat řádově výše než na běžný provoz
- Škálovatelná architektura (viz dále)
- Jako SW je jednou z možností Knot Resolver
 - spolehlivý
 - rychlý
 - modulární



Vysoká dostupnost

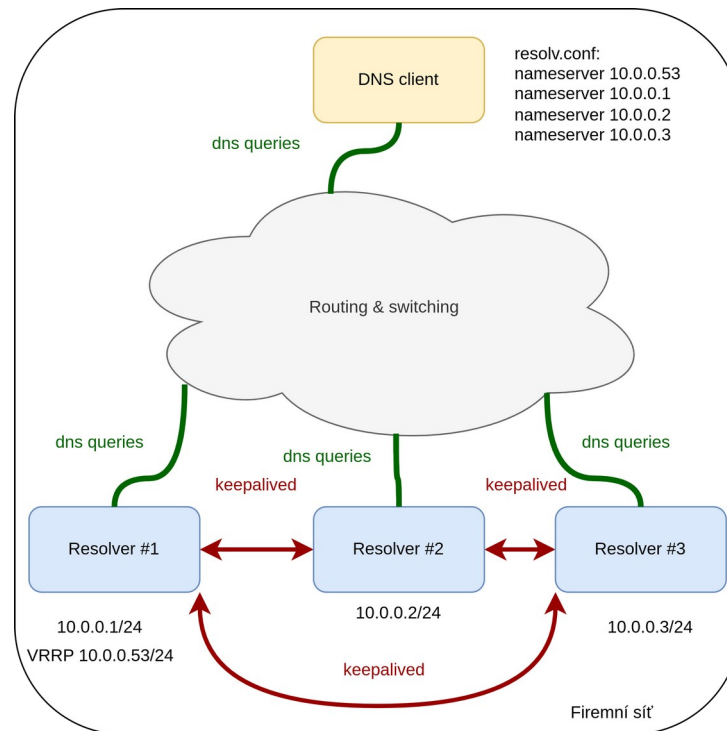
Vysoká dostupnost – více nezávislých instancí

- Závisí na klientovi
- Vytížen jen primární resolver
- Odstávka resolveru => timeoute DNS dotazů



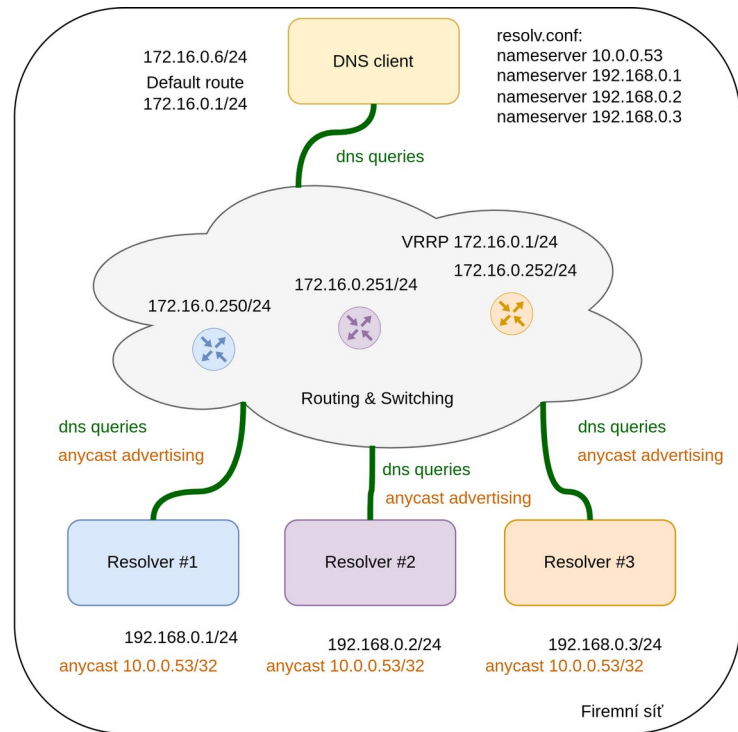
Vysoká dostupnost – VRRP/Keepalived

- Přehazování VIP adresy
- Potřeba restartu DNS démona
- Neškáluje - vytížený jen server s VIP adresou



Vysoká dostupnost – IP anycast

- Primární adresa IP anycast
- Vysoká škálovatelnost
- Vysoká redundance
- Geografická redundance
- Může být /32 a /128
- VXLAN a anycast VRRP



Filtrování hrozeb

- Máme do DNS zasahovat filtry?

Filtrování hrozeb

- Má to být standard nebo příplatková služba?

Filtrování hrozeb

- Plnění zákonných požadavků
- Ochrana uživatelů před závadnými doménami
- Stahování přímo ze zdroje nebo cron scripty
- Vlastní, veřejné i komerční zdroje deny listů
- Moduly na dynamické filtrování

```
1 local-data:
2   rpz:
3     - file: /tmp/adult.rpz
4       tags: [ adult ]
5     # security blocklist applied for everyone
6     - file: /tmp/security.rpz
7     - watchdog: auto
```

yaml ▼

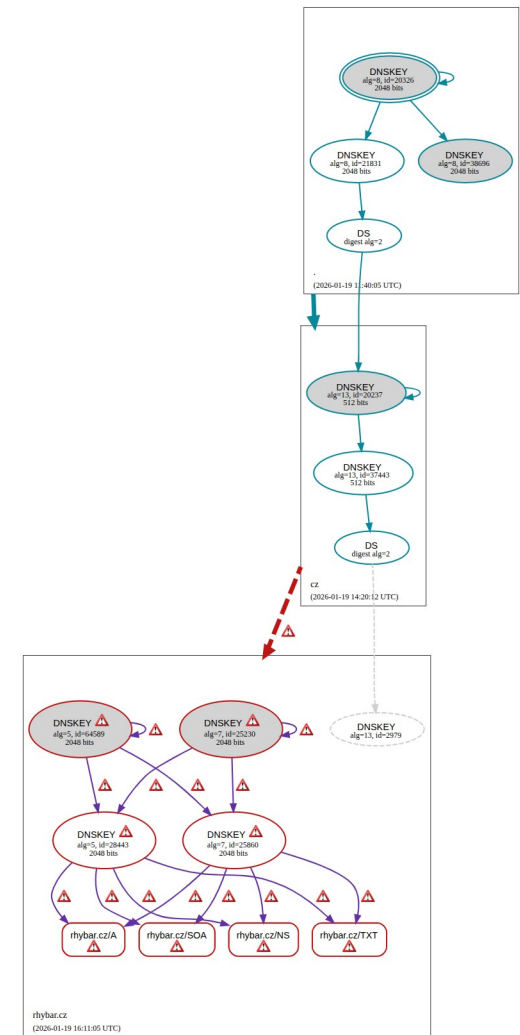
Rate Limiting

- Zamezení zneužívání vaší služby k odraženým útokům
- Ochrana služby samotné
- Omezení počtu dotazů z adresy, sítě
- DNS flood, DoS, DNS amplification útoky
- iptables, nft nebo knot-resolver
- Optimalizace paměti a CPU

```
1 rate-limiting:  
2   enable: true  
3   instant-limit: 100  
4   slip: 2  
5   rate-limit: 500
```

DNSSEC validace

- Dnes standardem, ale i tak se na něj zapomíná
- Ověření validity DNS záznamů



Soukromí

- Téměř veškerá komunikace se šifruje, ale DNS stále často ne
- Let's Encrypt certifikáty
- Častější rotace certifiátů
- Dig/kdig +https +tls

```
1 network:
2   listen:
3     - interface: &interfaces
4       - '<ip address>'
5       - '<ipv6 address>'
6     # DNS over TLS
7     - interface: *interfaces
8       kind: dot
9     # DNS over HTTPS
10    - interface: *interfaces
11      kind: doh2
12  tls:
13    cert-file: <path to cert>
14    key-file: <path to key>
```

Děkujeme vám za pozornost!

Tomáš Hála & Lukáš Vacek

• 21. 01. 2026

Odkazy



Denylisty.cz