

DNS PATROL

(Bezpečné DNS pro Kraj Vysočina)

Představení řečníků

- **Miroslav Hampl, CZ.NIC z.s.p.o.**
 - Business Development Manager v Laboratořích CZ.NIC

Co chceme? Resolver ...

- ... který bude sloužit pro bezpečný překlad externích domén,
- ... a který:
 - umožní správu, řízení, monitoring a analýzu DNS provozu
 - umožní detekci a blokaci hrozeb dle threat intelligence DB
 - detekci a blokaci DNS dotazů na základě whitelistingu a blacklistingu
 - detekci DGA dotazů a jiných anomálií
 - ...
- bezpečnostní nástroj
 - rychle a jednoduše implementovatelný
 - poměrně zajímavé výsledky s minimem úsilí

Přichází nová služba
z Laboratoří CZ.NIC



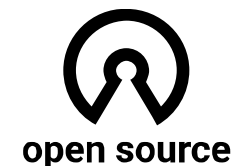
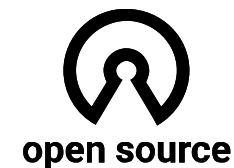
Ochrana vaší sítě před
kybernetickými hrozbami

Blokuje škodlivé domény

**Chrání před phishingem,
DGA, tunnelingem**

Threat Intelligence od CSIRT.CZ

Naše projekty – základ našeho řešení:



ODVR Statistiky

Instance resolverů - Statistiky denních průměrů QPS pro jednotlivé instance resolverů za posledních 30 dnů před 10.09.2025

Server	Max QPS	Min QPS	Trend	Průměr
s-01	3 044	1 700		2 288
r-01	2 898	1 717		2 260
b-01	2 922	1 700		2 254
b-03	2 804	1 690		2 209
b-02	1 667	1 033		1 277
b-04	1 613	994		1 266
s-02	1 715	846		1 243
r-02	1 664	129		905

Kódy odpovědí - Statistiky denních průměrů QPS pro odpovědi s daným kódem (RCODE) za posledních 30 dnů před 10.09.2025

RCODE	Max QPS	Min QPS	Trend	Průměr
NoError	13 477	7 317		10 218
NXDomain	3 241	1 110		1 734
ServFail	2 051	467		1 143
NotImp	452	37		180
Refused	109	84		97
YXDomain	0	0		0

Typy dotazů - Statistiky denních průměrů QPS pro dotazy s daným typem (QTYPE) za posledních 30 dnů před 10.09.2025

QTYPE	Max QPS	Min QPS	Trend	Průměr
A	7 962	4 843		6 595
AAAA	2 488	1 364		1 775

Top domény

Top 1000 domén podle DNS stupnice dne 09.09.2025 [i](#)

Filtrovat...

Pořadí Doména

- 1 google.com
- 2 gstatic.com
- 3 googleapis.com
- 4 apple.com
- 5 facebook.com
- 6 microsoft.com
- 7 akadns.net
- 8 test.dnscrypt
- 9 icloud.com
- 10 googleusercontent.com
- 11 akamai.net
- 12 doubleclick.net
- 13 aaplimg.com
- 14 live.com
- 15 office.com
- 16 in-addr.arpa
- 17 akamaiedge.net
- 18 apple-dns.net
- 19 whatsapp.net
- 20 seznam.cz

Zkušenosti převedené do našeho řešení

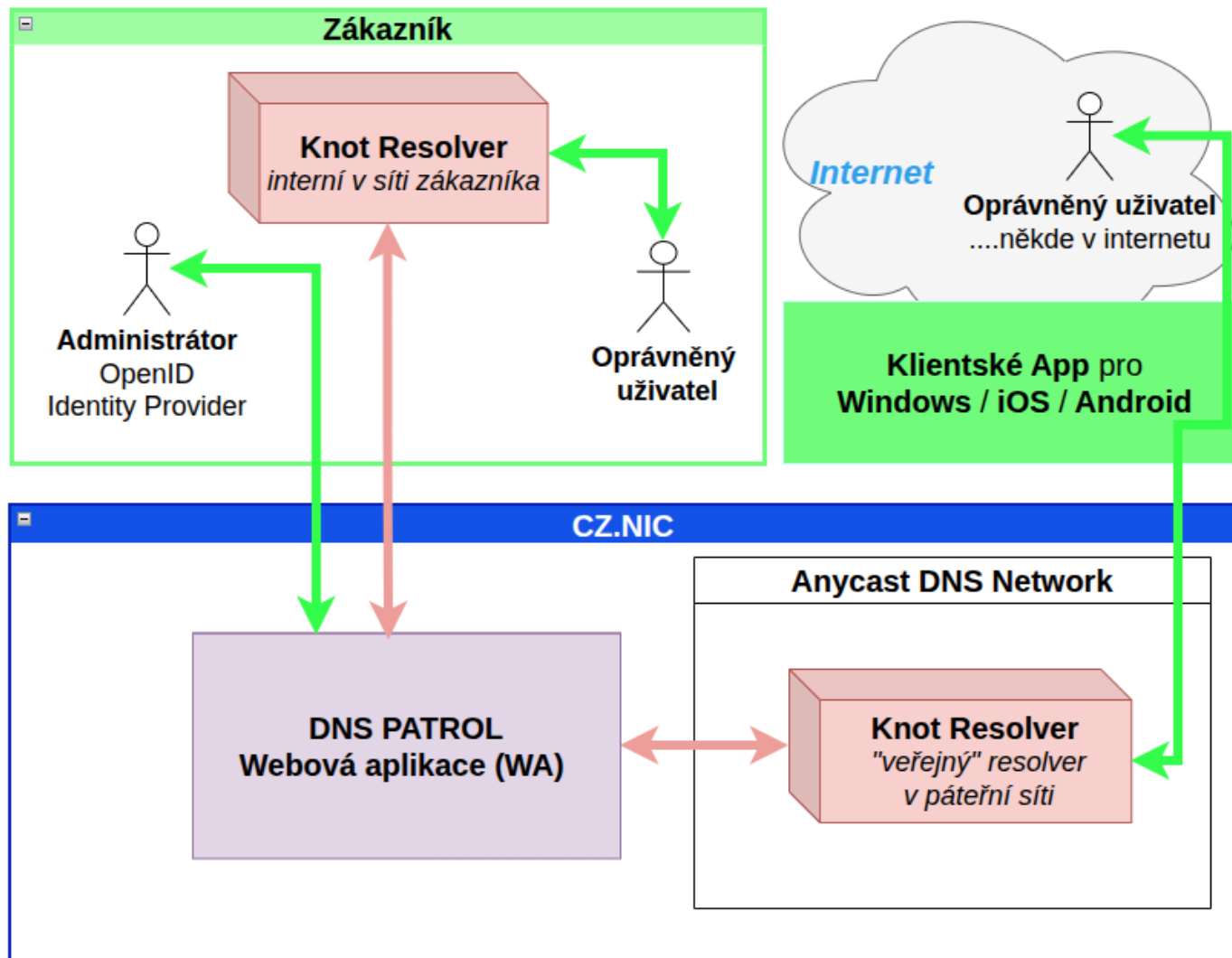
- 1)   **KNOT RESOLVER** - upraven na míru.
- 2) Oddělená anycastová infrastruktura.

Nové aplikace:

- 3)  **Administrativní portál WA** (Webová Aplikace).
 - Plně přizpůsobitelné rozhraní pro správce systému.
 - Log management:
 - Systém umožňuje nastavení fungování na blokování a auditing pro jednotlivé vrstvy.
 - Systém také umožňuje zpětnou analýzu DNS provozu:
- 4)  **Klientské aplikace** pro **Windows** / **iOS** / **Android**.

DNS PATROL

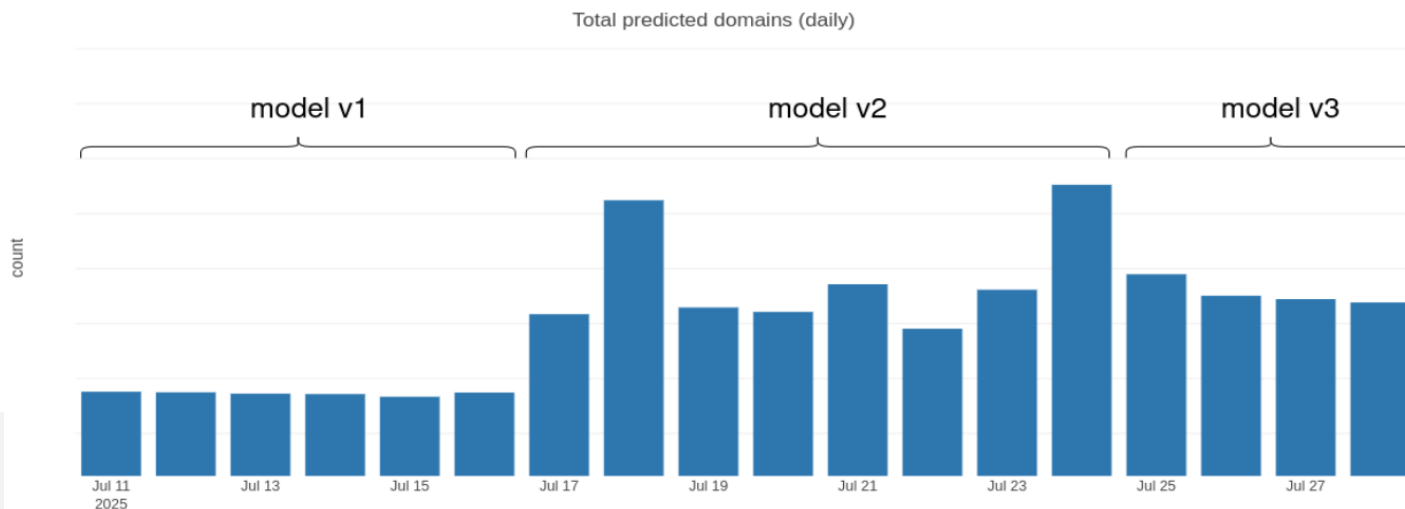
Přehledová architektura



Nové moduly a nástroje

Analytický modul (ML - Machine Learning)

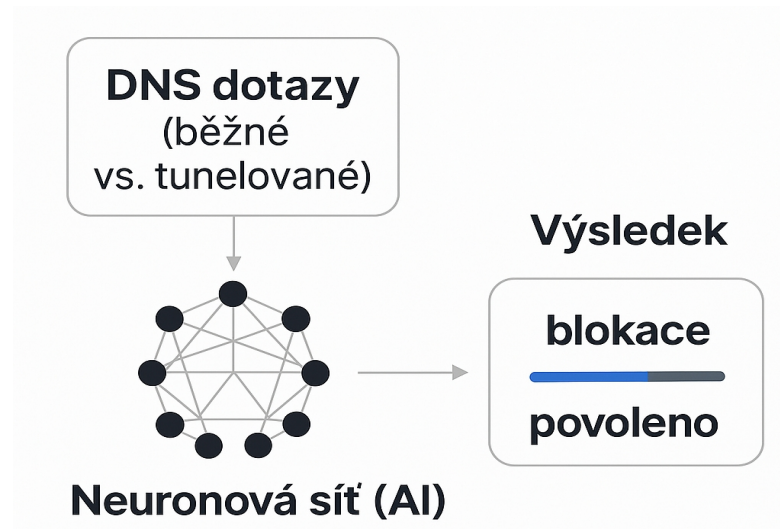
- Strojové učení nad Passive DNS, které analyzuje historická DNS data za účelem detekce škodlivých domén.
 - Přesnost je změřená metrikou Accuracy na testovací sadě (jaká je míra úspěšnosti).
 - Modul třetí generace dosahuje přesnosti 98 % na testovací sadě.



Nové moduly a nástroje

Behaviorální moduly zaměřené na hrozby:

- **DNS tunneling** – pro tento účel jsme vyvinuli speciálně naučenou Neuronovou síť.
- **Zero-Day útoky (DGA)** - detekce nově vzniklých domén, které útočníci používají jako **Command & Control servery** pro malware.



Deny Listy – Threat Intelligence Database (CZ.NIC)

- Komerčně dostupné od 2024.

Nové moduly a nástroje

Filtrační moduly, zpracovávají tyto hrozby:

- Modul pro detekci phishingových a homografických útoků.
- Modul pro detekci **cílených** phishingových a homografických útoků
 - Aktuální verze už našla doménu pátého řádu, která byla předána k řešení:

mail2.kr-vysocina.cz.club

Děkuji vám za pozornost!

Miroslav Hampl – miroslav.hampl@nic.cz