DNS PATROL

neboli

bezpečné DNS pro Kraj Vysočina

Miroslav Hampl • 21.01.2026

CZ.NIC | SPRÁVCE DOMÉNY CZ

Očekávání Kraje Vysočina od nové DNS služby:

Aktivity v oblasti kyberbezpečnosti

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

Kraj Vysočina 2 Dominik Marek

Jak navrhnout bezpečnostní řešení správně

Vlevo - **Ucelené řešení:**

- ✔ jasný kontext
- ✔ předvídatelné chování
- ✔ připravené pro provoz

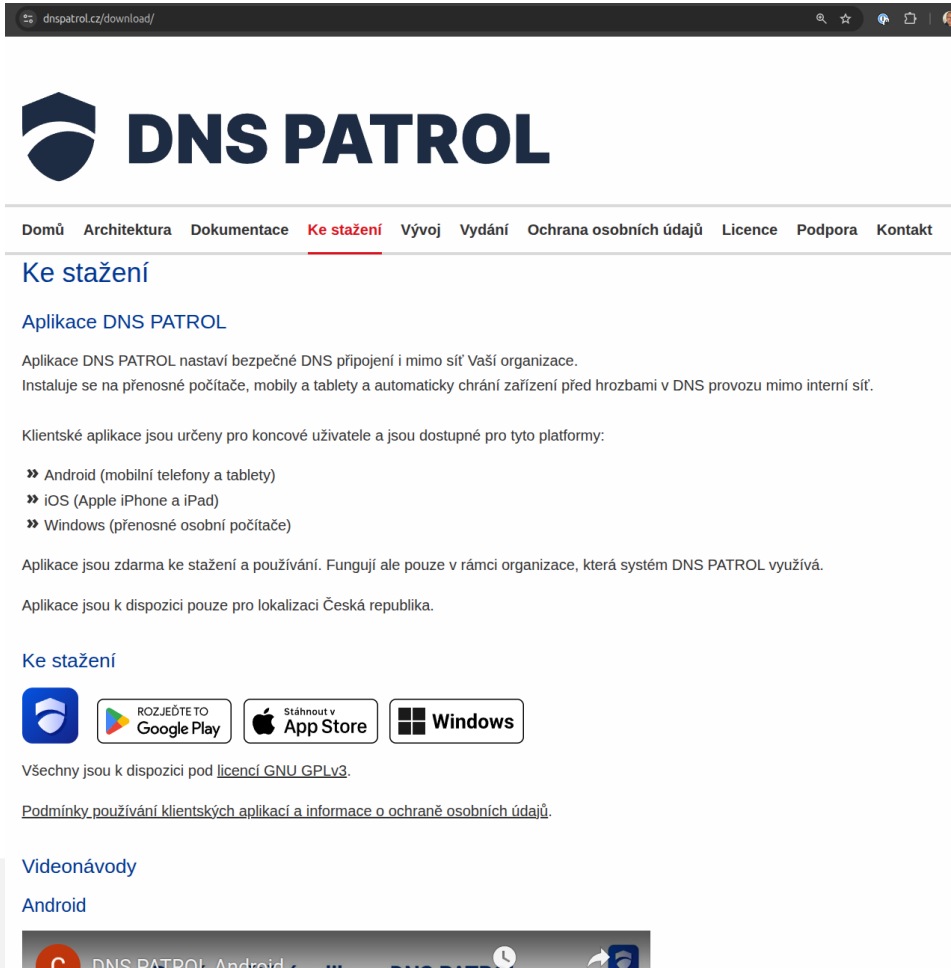
Vpravo - **Sada komponent:**

- ✗ chybí kontext
- ✗ ruční integrace
- ✗ riziko slepých míst

DNS PATROL je navržen jako ucelený systém, ne jako sbírka nástrojů.

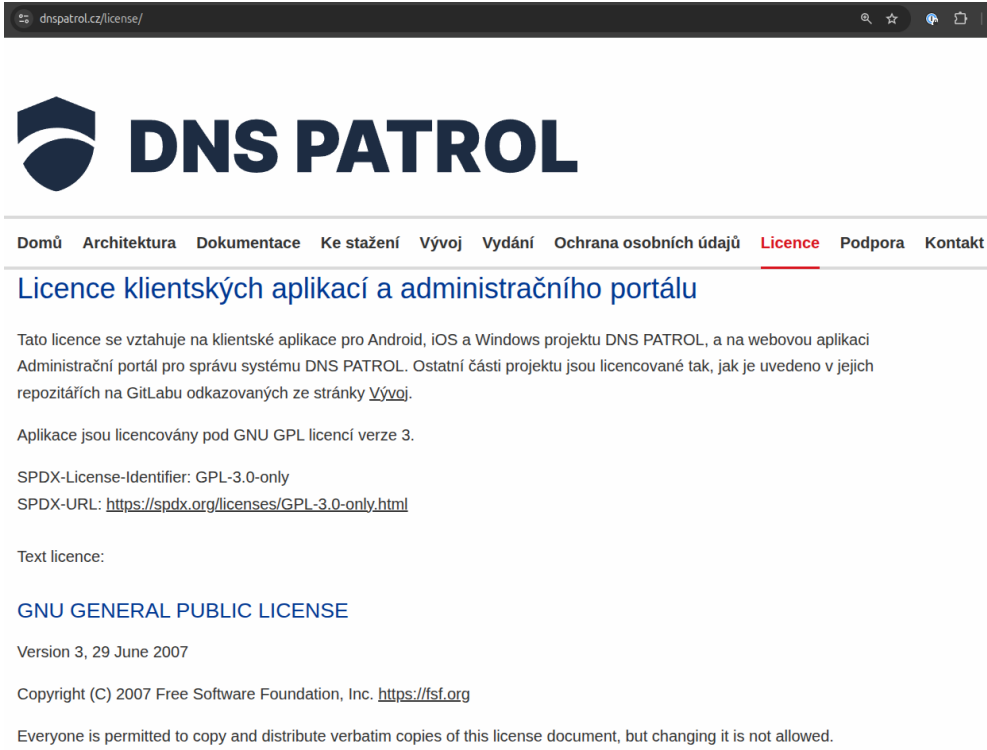
Vývoj nových nástrojů na základě dlouhodobých zkušeností

1) Upravený KNOT RESOLVER
2) Oddělená anycastová infrastruktura
3) Nová webová aplikace:
   - administrativní portál pro správu systému
   - centrální log management s podporou blokování a auditního režimu
4) Nové klientské aplikace pro **Windows**, **iOS** a **Android**
5) Podrobnosti na: www.dnspatrol.cz

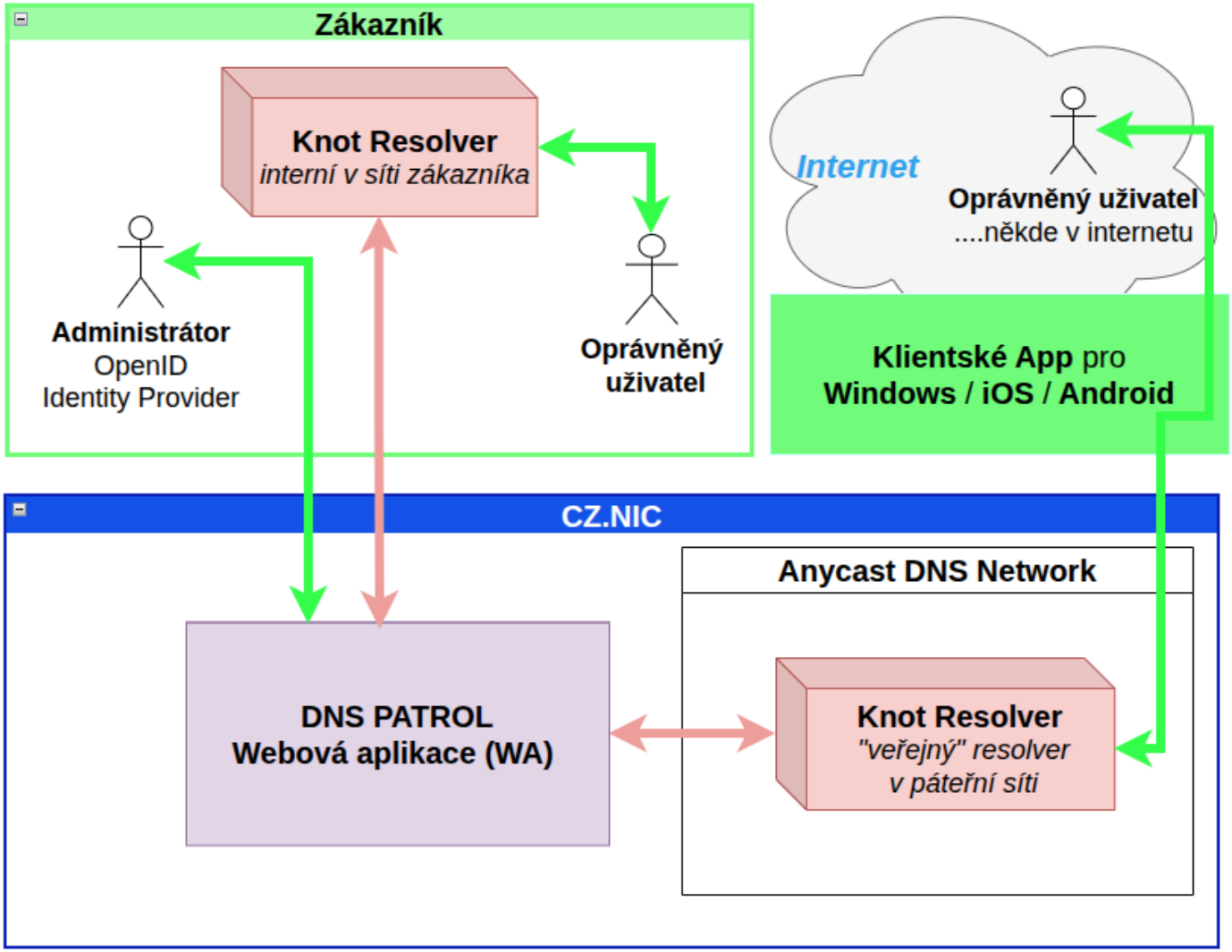


Licenční model řešení

- DNS PATROL je dostupný pod licencí **GNU GPL v3**
- Zdrojové kódy jsou veřejně dostupné



DNS PATROL
Přehledová architektura



DNS PATROL a RPZ zóny

Jak vznikají blacklisty a whitelisty

- Každý modul řeší konkrétní typ hrozby nebo výjimky a jeho výstupem je samostatná RPZ zóna, což umožňuje definovat individuální bezpečnostní politiky pro různé části sítě
- Každá RPZ zóna má nezávislý provozní režim
  - **aktivně uplatněny** v bezpečnostní politice,
  - použity **pouze pro audit** a vyhodnocování,
  - nebo **zcela vypnuty**.
- White listy mají **vyšší prioritu** a slouží k řízeným výjimkám a potlačení falešných pozitivních detekcí.

Průběžná aktualizace a zdroje dat

Živý systém, nikoliv statické seznamy

- Moduly a RPZ zóny jsou **průběžně aktualizovány.**
- Aktualizace vychází z:
  - reálného DNS provozu,
  - pasivního DNS,
  - threat intelligence databází,
  - strojového učení a detekce anomálií.
- Vlastní blacklisty DNS PATROL vznikají na základě **detekce chování**, ne pouze převzatých seznamů.
- Externí blocklisty z veřejných zdrojů jsou:
  - volitelným doplňkem,
  - jasně oddělené od vlastních modulů.

Moduly vytvářené ve sdružení CZ.NIC

001-010 - Whitelisty (seznamy bezpečných domén)

- **001nic-wl-cze-adam** — bezpečné .CZ domény (CZ.NIC ADAM)
  - *důvěryhodné zdroje z ČR, jako jsou státní domény, apod.*
- ***002nic-wl-world-adam*** — bezpečné celosvětové domény (CZ.NIC ADAM)
  - *důvěryhodné evropské a mezinárodní zdroje, s důrazem na EU*
- ***003nic-wl-ti-denylisty*** — bezpečné domény (CZ.NIC Deny Listy)
  - *naše Threat Intelligence databáze*
- ***004nic-wl-proverene*** — bezpečné domény (prověřené z dříve blokovaných)
  - ručně prověřené domény

Moduly vytvářené ve sdružení CZ.NIC

800–899 - Blacklisty

- ***801nic-bl-zakonne*** — zákonné blacklisty vycházející z legislativních povinností v ČR
- ***802nic-bl-tidb-denylisty*** — domény z Threat Intelligence databáze (CZ.NIC Deny Listy)
- ***803nic-bl-akt-v-podezreni*** — domény detekované jako aktuálně podezřelé
- ***804nic-bl-cileny-phishing*** — domény detekované jako cílený phishing na domény Kraje Vysočina
- ***805nic-bl-obecny-phishing*** — domény detekované jako obecný phishing a homografy (CZ.NIC Deny Listy)
- ***806nic-bl-dga*** — domény detekované jako zero-day útoky (DGA)
- ***807nic-bl-ns-dns-tunneling*** — Neuronová síť–výstup ML modelu z resolverů detekující DNS tunneling
- ***808nic-bl-ml-passive-dns*** — výstup interního ML modelu nad systémem passive DNS
- ***809nic-bl-neeticke-eshopy*** — domény s neetickými eshopy (přeprodej dálničních známek, apod.)

901 – 999 Blacklisty z externích zdrojů

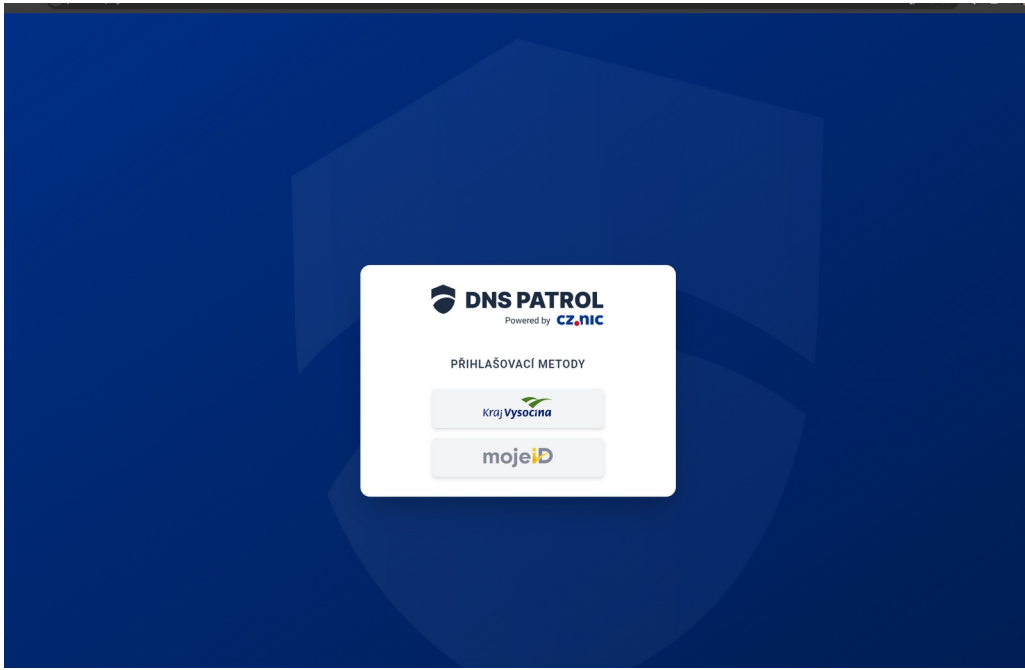
DNS PATROL powered by CZ.NIC

(Sdružení CZ.NIC nenese odpovědnost za úplnost, správnost ani aktuálnost informací obsažených v těchto modulech.)

- ***915ext-bl-tiktok*** — domény TikToku a propojených služeb
- ***905ext-bl-facebook*** — domény Facebooku a propojených služeb
- ***911ext-bl-adult-content*** — weby s obsahem pro dospělé
- ***901ext-bl-zneuz-zranitelnost*** — weby zneužívající zranitelnosti systému
- ***902ex-bl-reklamni-srv*** — reklamní servery
- ***903ext-bl-crypto*** — kryptoměnové weby (může blokovat i legitimní stránky)
- ***904ext-bl-nelegalni-drogy*** — weby týkající se nelegálních drog
- ***907ext-bl-hazardni-hry*** — weby s hazardními hrami
- ***909ext-bl-world-phishing*** — phishingové weby
- **…**
- ***917ext-bl-sledovani-users*** — weby určené k sledování a uchovávání dat uživatelů

Administrativní portál (WA) – autentizace

- Webové rozhraní pro přihlášení do DNS PATROL
- Přihlášení realizované pomocí OIDC
  - Min. úroveň záruky značná
    - Vysočina ID
    - MojeID



DNS PATROL
Powered by cz.nic

Miroslav Hampl
Super User

Přehled

Nastavení DNS

Nastavení přístupu

Analytika

Nastavení

O aplikaci

Odhlásit

Vítejte na hlavní stránce

DNS PATROL

Miroslav Hampl
Super User

- Přehled
- Nastavení DNS
  - Zóny
  - **Resolvery**
  - Podsítě
  - Sady pravidel
- Nastavení přístupu
- Analytika
- Nastavení
- O aplikaci
- Odhlásit

Resolvery

Hostname ↓	Zóna	IPv4 adresy	IPv6 adresy	Master resolver	Stav	Poslední kontrola	
Filtr...	Filtr...	Filtr...	Filtr...	Vše	Vše	DD . MM . RRRR HH : mm	
dns-ext-01	EXT	192.0.2.53	2001:db8::53		OK	13. 01. 2026 15:05:02 SEČ	OK
dns-ext-02	EXT	192.0.2.54	2001:db8::54		OK	13. 01. 2026 15:05:02 SEČ	OK
dns-net01-01	NET01	198.51.100.53	2001:db8:1::53		OK	13. 01. 2026 15:05:02 SEČ	OK
dns-net01-02	NET01	198.51.100.54	2001:db8:1::54		OK	13. 01. 2026 15:05:01 SEČ	OK

DNS PATROL
Powered by CZ.NIC

Miroslav Hampl
Super User

- Přehled
- Nastavení DNS
  - Zóny
  - Resolvery
  - Podsítě
  - **Sady pravidel**
- Nastavení přístupu
- Analytika
- Nastavení
- O aplikaci
- Odhlásit

Sady pravidel

+ Přidat sadu pravidel

Jméno ↑	Popis	Typ sady pravidel	Zdroj
Filtr...	Filtr...	Vše	Filtr...
001nic-wl-cze-adam	Whitelist internal safe domains CZ ADAM	Whitelist	cz.nic
002nic-wl-world-adam	Whitelist internal safe domains world ADAM	Whitelist	cz.nic
003nic-wl-ti-denylisty	Whitelist internal safe domains CZ DENY LISTY	Whitelist	cz.nic
004nic-wl-proverene	Whitelist with false positive domains	Whitelist	cz.nic
701nemocnicepraha	Nemocnice Praha fiktivni	Blocklist	internal
801nic-bl-zakonne	Zákonné blacklisty / Typ hrozby: ALL – všechny hrozby	Blocklist	cz.nic
802nic-bl-tidb-denylisty	Deny listy - Threat Intelligence databáze / Typ hrozby: ALL – všechny hrozby	Blocklist	cz.nic
803nic-bl-akt-v-podezreni	Modul detekující aktuálně podezřelé domény z laboratoří CZ.NIC / Typ hrozby: ALL – všechny hrozby	Blocklist	cz.nic
804nic-bl-cileny-phishing	Modul detekující cílený Phishing na domény kraje / Typ hrozby: Phishing	Blocklist	cz.nic
805nic-bl-obecny-phishing	Modul detekující obecný Phishing a homografy / Typ hrozby: Phishing	Blocklist	cz.nic

Strana 1 z 4

Zobrazit 10

DNS PATROL
Powered by CZ.NIC

Miroslav Hampl
Super User

- Přehled
- Nastavení DNS
  - Zóny
  - Resolvery
  - **Podsítě**
  - Sady pravidel
- Nastavení přístupu
- Analytika
- Nastavení
- O aplikaci
- Odhlásit

Podsítě

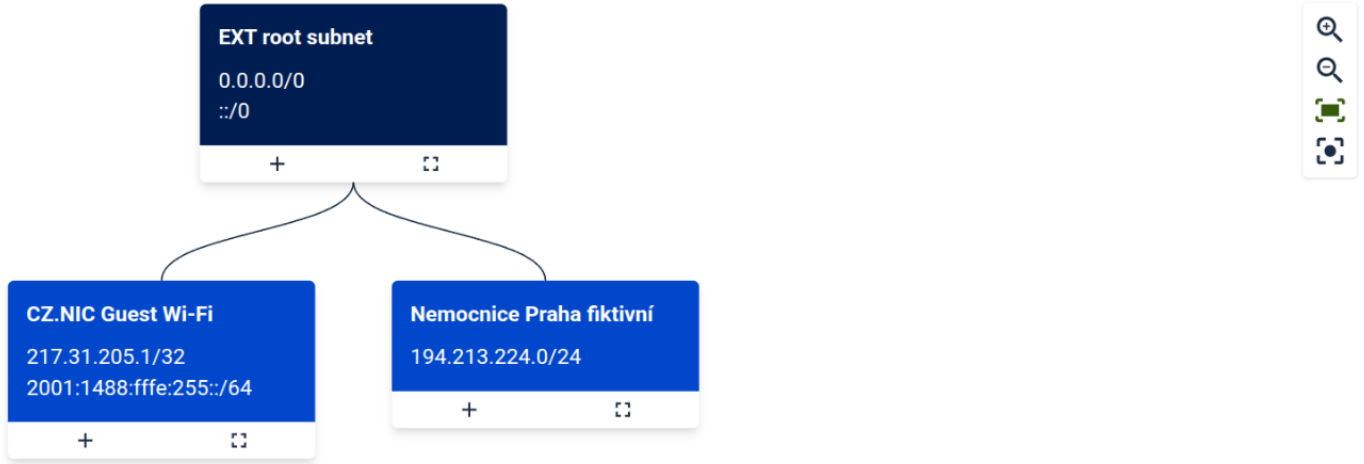
+ Přidat podsíť

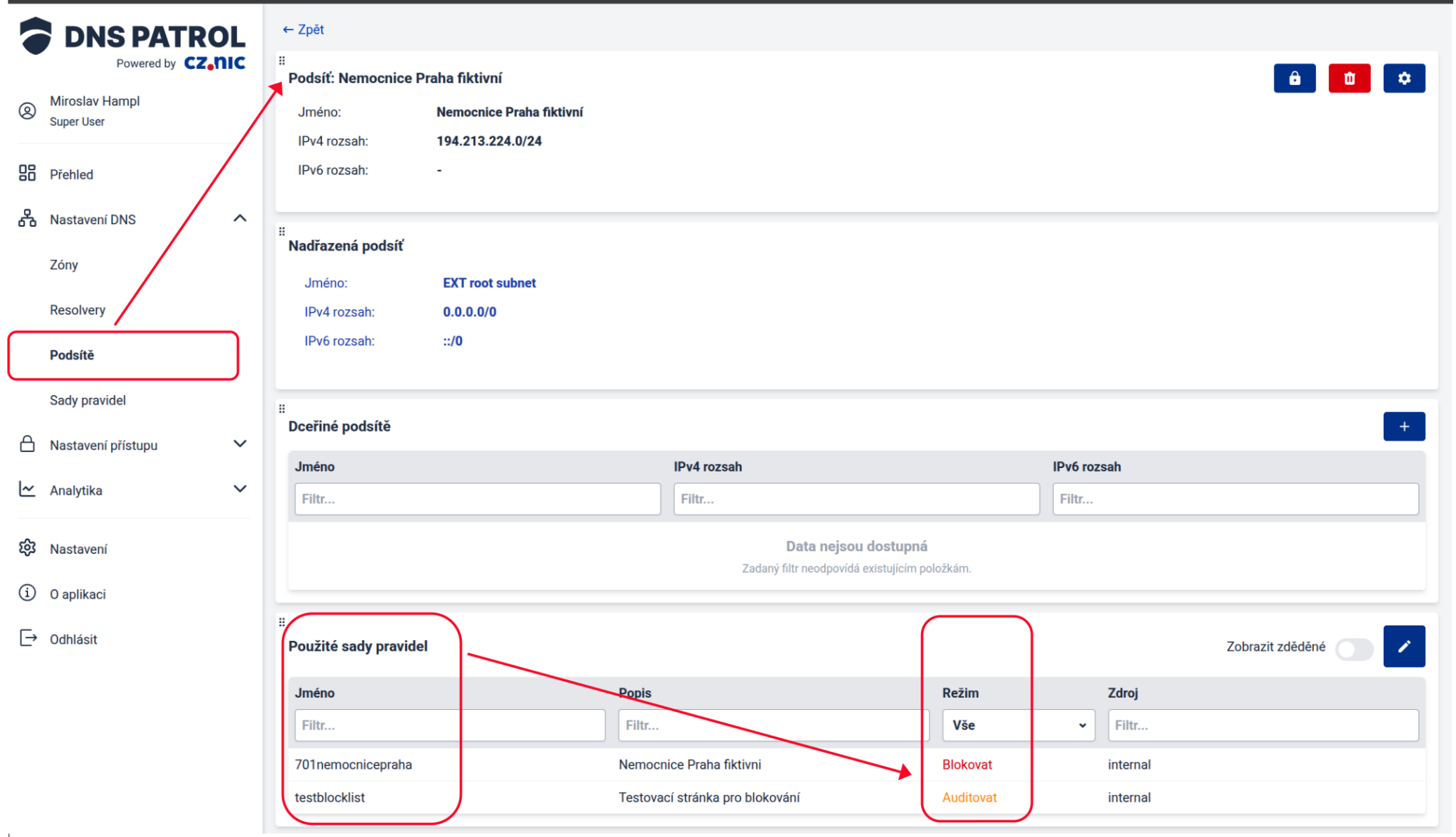
Jméno ↓	IPv4 rozsah	IPv6 rozsah	Nadřazená podsíť
Filtr...	Filtr...	Filtr...	Filtr...
ROWANET root subnet	0.0.0.0/0	::/0	-
Nemocnice Praha fiktivní	194.213.224.0/24	-	EXT root subnet
CZ.NIC Guest Wi-Fi	217.31.205.1/32	2001:1488:fffe:255::/64	EXT root subnet

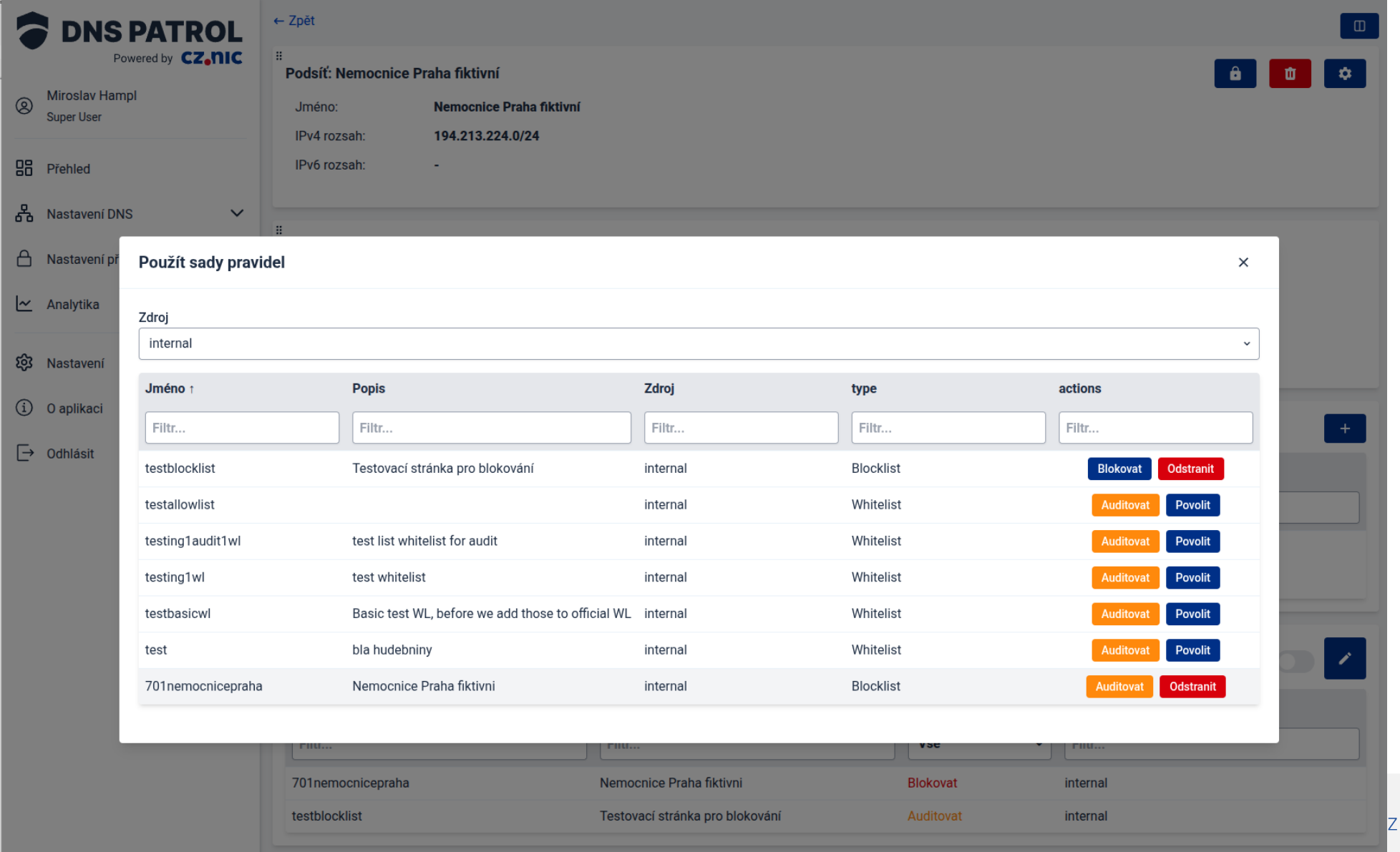
‹ Strana 1 z 1 › Zobrazit 10

Struktura podsítě

Upravit strukturu sítě | Rozložení grafů | Jednotlivé kořeny




DNS PATROL
Powered by CZ.NIC
Miroslav Hampl
Super User
Přehled
Nastavení DNS
Zóny
Resolvery
Podsítě
Sady pravidel
Nastavení přístupu
Analytika
Nastavení
O aplikaci
Odhlásit
← Zpět
Podsíť: Nemocnice Praha fiktivní
Jméno: Nemocnice Praha fiktivní
IPv4 rozsah: 194.213.224.0/24
IPv6 rozsah: -
Nadřazená podsíť
Jméno: EXT root subnet
IPv4 rozsah: 0.0.0.0/0
IPv6 rozsah: ::/0
Dceřiné podsítě
Jméno
IPv4 rozsah
IPv6 rozsah
Filtr...
Data nejsou dostupná
Zadaný filtr neodpovídá existujícím položkám.
Použité sady pravidel
Zobrazit zděděné
Jméno
Popis
Režim
Zdroj
Vše
701nemocnicepraha
Nemocnice Praha fiktivni
Blokovat
internal
testblocklist
Testovací stránka pro blokování
Auditovat
internal


DNS PATROL
Powered by cz.nic
Miroslav Hampl
Super User
Přehled
Nastavení DNS
Nastavení př
Analytika
Nastavení
O aplikaci
Odhlásit
← Zpět
Podsíť: Nemocnice Praha fiktivní
Jméno: Nemocnice Praha fiktivní
IPv4 rozsah: 194.213.224.0/24
IPv6 rozsah: -
Použít sady pravidel
Zdroj
internal
Jméno ↑
Popis
Zdroj
type
actions
Filtr...
testblocklist Testovací stránka pro blokování internal Blocklist Blokovat Odstranit
testallowlist internal Whitelist Auditovat Povolit
testing1audit1wl test list whitelist for audit internal Whitelist Auditovat Povolit
testing1wl test whitelist internal Whitelist Auditovat Povolit
testbasicwl Basic test WL, before we add those to official WL internal Whitelist Auditovat Povolit
test bla hudebniny internal Whitelist Auditovat Povolit
701nemocnicepraha Nemocnice Praha fiktivni internal Blocklist Auditovat Odstranit
701nemocnicepraha Nemocnice Praha fiktivni Blokovat internal
testblocklist Testovací stránka pro blokování Auditovat internal

DNS PATROL
Powered by CZ.NIC

Miroslav Hampl
Super User

- Přehled
- Nastavení DNS
- Nastavení přístupu
- Analytika
  - **Statistiky**
  - Historie záznamů
  - Pasivní DNS
  - Soubory
- Nastavení
- O aplikaci
- Odhlásit

Statistiky

Skrýt filtry

Ukázková data z testovacího prostředí.

☑ Synchronizovat krok

Krok: Den

☑ Synchronizovat datumy

Od data: 01.10.2025, 11:46

Do data: 31.10.2025, 11:46

☑ Synchronizovat filtry

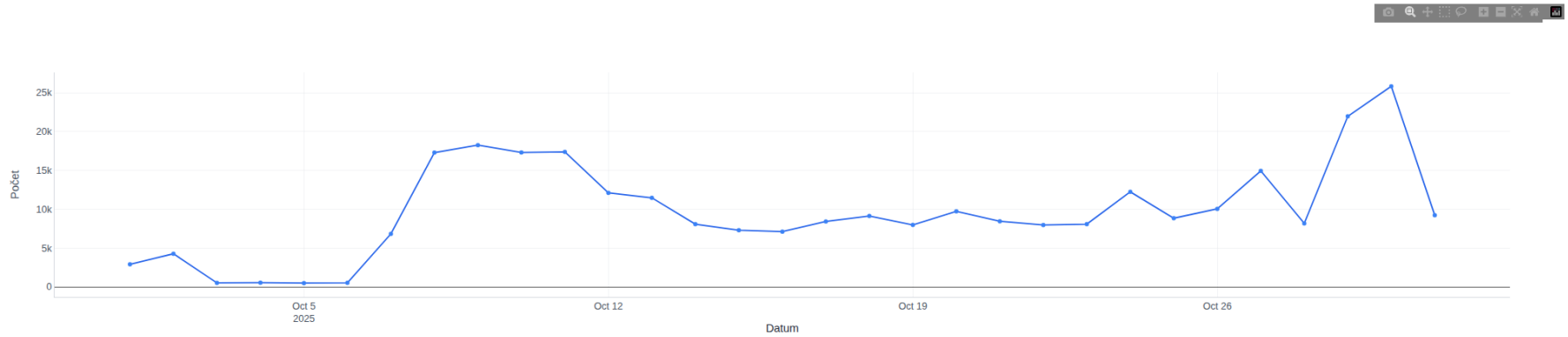
Resolver: Vybráno: 1

Doména: Zadejte doménu

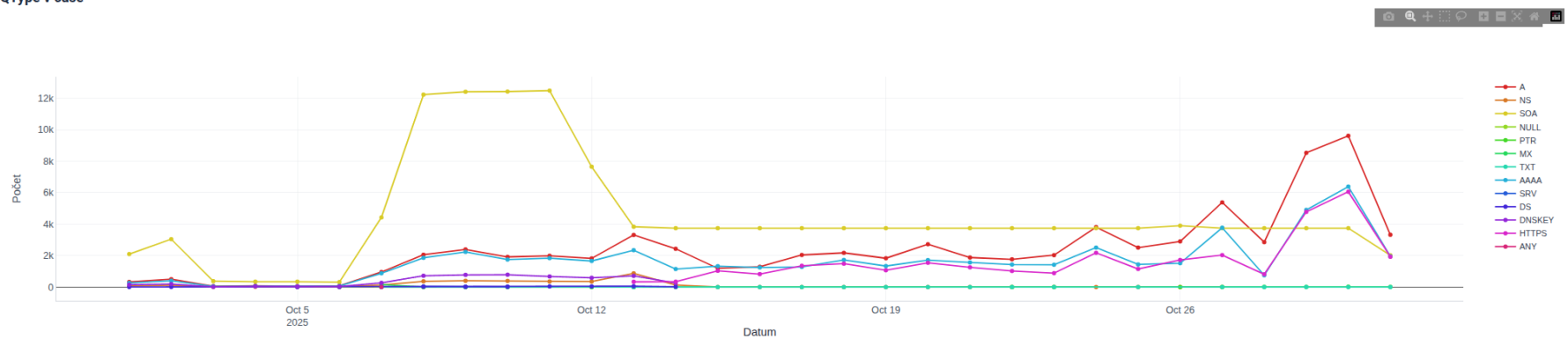
IP: Zadejte IP adresu

Země: Vše

Počet dotazů



QType v čase



DNS PATROL
Powered by cz.nic

Miroslav Hampl
Super User

- Přehled
- Nastavení DNS
- Nastavení přístupu
- Analytika
  - **Statistiky**
  - Historie záznamů
  - Pasivní DNS
  - Soubory
- Nastavení
- O aplikaci
- Odhlásit

Nejčastější domény

1	nic.cz
2	cz
3	udp53.cz
4	google.com
5	apple.com

8

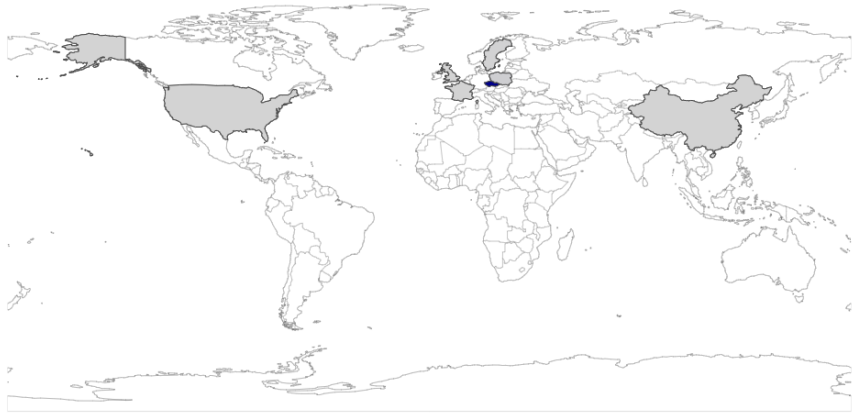
Ukázková data z testovacího prostředí.

Nejčastější zdroje

Limit 5

1	217.31.207.162	46
2	217.31.207.206	40
3	185.43.135.100	27
4	2001:148f:fffe::100	27
5	2001:1488:91::2	17

Distribuce podle země



Nejčastější resolvery

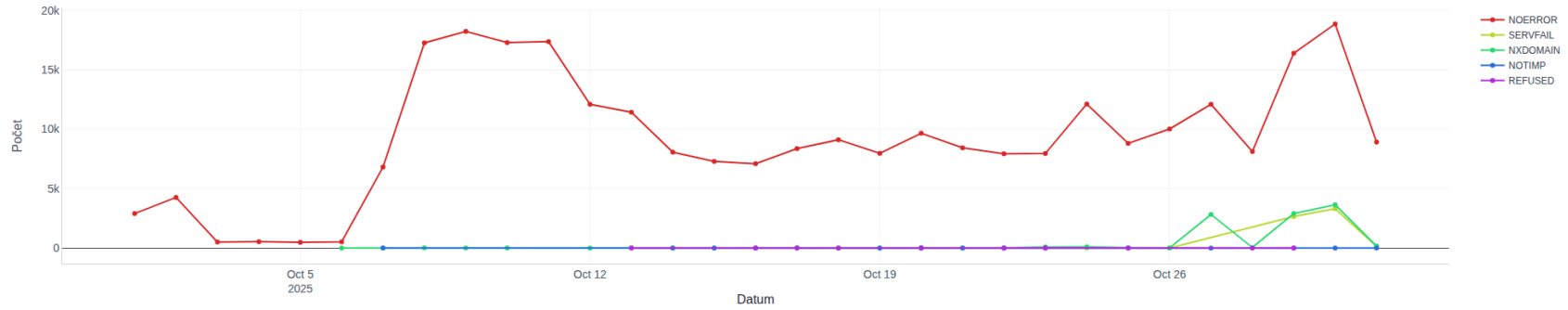
Limit 5

DNS PATROL
Powered by CZ.NIC

Miroslav Hampl
Super User

- Přehled
- Nastavení DNS
- Nastavení přístupu
- Analytika
  - **Statistiky**
  - Historie záznamů
  - Pasivní DNS
  - Soubory
- Nastavení
- O aplikaci
- Odhlásit

Distribuce RCode v čase



Akce zásad

Akce zásad podle pravidla

Ukázková data z testovacího prostředí.

Miroslav Hampl
Super User

Přehled
Nastavení DNS
Nastavení přístupu
Analytika
Statistiky
Historie záznamů
Pasivní DNS
Soubory
Nastavení
O aplikaci
Odhlásit

Konstruktor dotazů

Rozšířený režim

Podmínky

Server	eq	odvr-jezek-s-01 (EXT)
AND		
Název DNS dotazu	eq	nic.cz
AND		
Datum a čas (místní)	gte	02.01.2026 15:03
AND		
Datum a čas (místní)	lte	14.01.2026 15:05

Seřadit podle

Vybráno: 1

`Datum a čas (místní)`

Zobrazení vyhledávání (SQL):

```
SELECT *
WHERE Server = 'odvr-jezek-s-01'
  AND Název DNS dotazu = 'nic.cz'
  AND Datum a čas (místní) >= 1767362580
  AND Datum a čas (místní) <= 1768399500
ORDER BY Datum a čas (místní) DESC
LIMIT 100;
```

Hledat | Resetovat

Limit: 100

Děkuji vám za pozornost!

Miroslav Hampl – miroslav.hampl@nic.cz