DNS PATROL

powered by CZ.NIC

DNS PATROL

Dokumentace

PRO VERZI
1.0.6

AKTUALIZOVÁNO
24. 9. 2026

ONLINE
labs.pages.nic.cz/dnspatrol-docs ↗

Obsah

01

Přehled

Vítejte v dokumentaci pro DNS PATROL! DNS PATROL je systém umožňující organizacím zabezpečit a monitorovat DNS provoz na své síti. Administrátoři mohou použít webový portál k nastavení politik jednotlivých podsítí, správu uživatelů, či monitorování a analýze provozu. Koncoví uživatelé se díky klientským aplikacím vždy připojí k správnému DNS resolveru.

1.1 Obsah

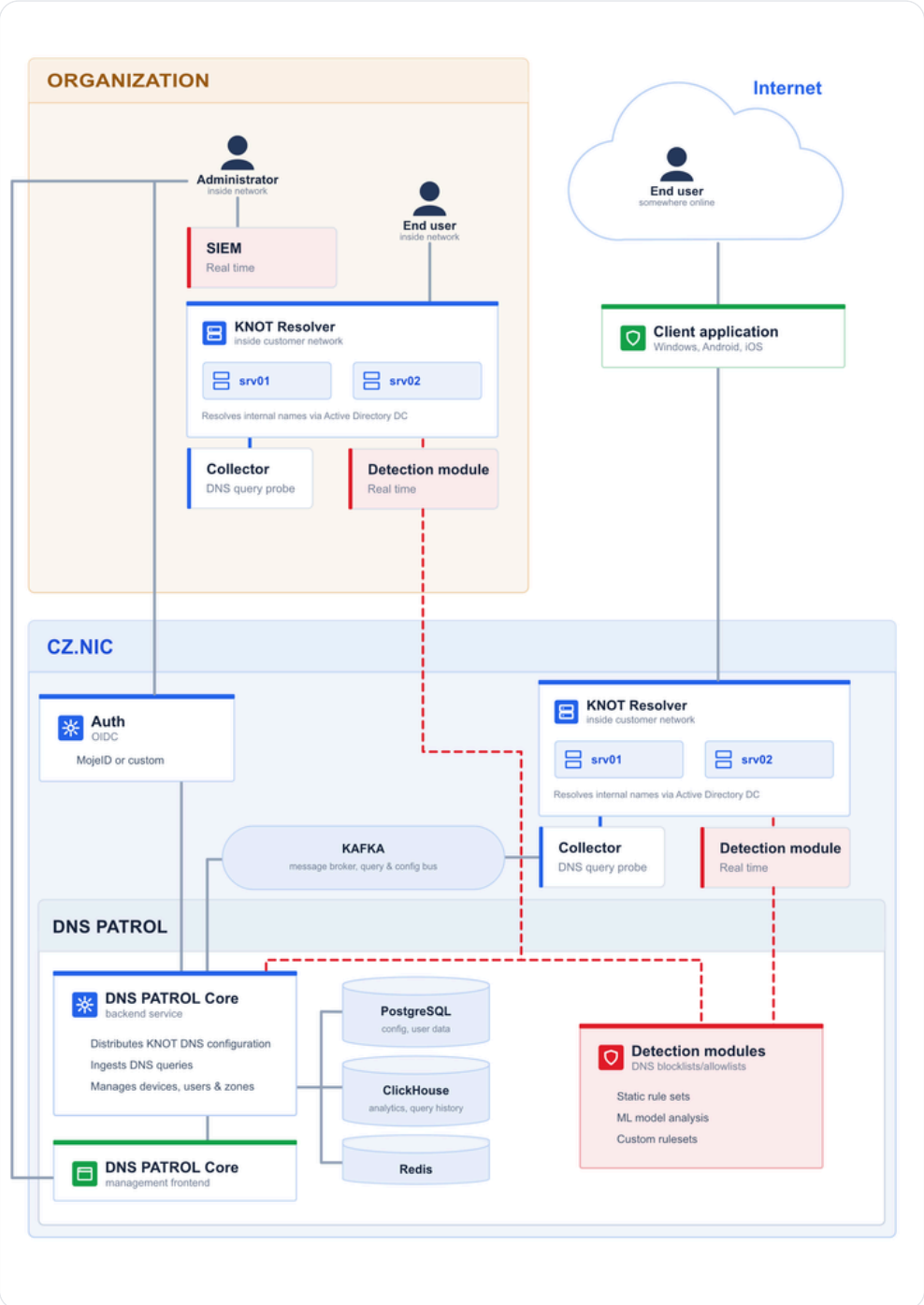
02

Infrastruktura

DNS PATROL je systém sestávající se z typicky několika resolverů, z nichž některé mohou být přímo uvnitř sítě organizace. Tyto resolvery získávají svoji konfiguraci z backendu, který je ovládán skrze administrátorský webový portál. Resolvery posílají data o dotazech do databáze, se kterou pro účely analýzy dat komunikuje i webový portál.

2.1 Systémy

Tato sekce popisuje jednotlivé komponenty systému DNS PATROL.



Obrázek 1 Architektura DNS PATROL: komponenty v síti organizace a v infrastruktuře CZ.NIC.

Resolvery

DNS dotazy se vyhodnocují instancemi KNOT Resolveru ↗. Resolver se může nacházet ve vnitřní síti organizace, kde zároveň komunikuje s Active Directory Domain Controller pro resolvování interních domén. Pro podsítě v rámci širší firemní sítě lze nasadit další resolvery. Pro koncové zařízení mimo síť organizace existuje externí resolver, na který se dotazuje pomocí unikátních DoH URL.

Vedle resolveru běží kolektor, který zachycuje informace o všech vyhodnocených dotazech a publikuje je do Kafky.

Kafka

Kafka ↗ slouží jako prostředník komunikace mezi resolvery a službami backendu. Slouží také jako krátkodobá záloha DNS dotazů v případě selhání hlavní databáze.

Komunikace je obousměrná, resolvery do Kafky publikují záznamy o dotazech a z Kafky odebírají konfigurační soubory (zóny, blacklisty a další pravidla), který dodává jádro podle aktuálního nastavení v portálu.

DNS PATROL Core

Jádro systému ovládané skrze administrátorský panel. Skrze Kafku aktualizuje podle aktuálního nastavení konfiguraci resolverů a v živém režimu přijímá DNS dotazy. Do databází ukládá informace o nastavení systému, nebo se dotazuje na dlouhodobé analytické informace. Autentizaci uživatelů zajišťují externí OpenID ↗ provideři, jako například Moje ID ↗.

Pro rychlé dohledání zaregistrovaných zařízení a zón používá jádro Redis cache, do které zapisuje při každé změně registrovaných zařízení nebo konfigurace.

Backend může posílat audit akcí administrátorů v portálu do externích informačních systémů protokolem syslog, typicky pro integraci s firemním SIEM.

Administrátorský panel

Administrátorský panel je webová aplikace, jejíž používání je detailně popsáno v sekci Webový portál.

Databáze

PostgreSQL ↗ – Struktura sítě, uživatelé, zařízení a konfigurace politik, atp.

ClickHouse ↗ – Slouží k zpracování velkého množství analytických dat. Drží historii dotazů pro statistiky a vyhledávání v portálu.

Redis ↗ – In-memory cache zaregistrovaných zařízení a zón pro nízkolatenční vyhledávání.

Koncové zařízení

Koncová zařízení používající externí resolver se do systému přihlašují pomocí klientské aplikace a jednorázového registračního kódu vystaveného z administrátorského portálu.

Klientská aplikace na zařízení odešle registrační kód spolu s hostname, MAC adresou a informacemi o operačním systému do DNS PATROL Core. Ten kód ověří, vytvoří nový záznam o zařízení svázaný s uživatelem, kterému kód patří, a vrátí klientovi identifikační token a unikátní DoH URL. Na tuto URL pak zařízení směruje všechny DNS dotazy.

2.2 Zóny, podsítě a sady pravidel

Logické členění sítě a politik v DNS PATROL stojí na třech entitách. Zóna je nejvyšší celek a sdružuje skupinu resolverů. Uvnitř zóny tvoří podsítě stromovou hierarchii podle adresního rozsahu. Na podsítě se navazují sady pravidel, které určují, jaké DNS dotazy se v daném místě hierarchie povolují, blokují nebo jen auditují.

Zóny

Zóna sdružuje skupinu resolverů spravovaných pod jednou konfigurací. Zóna může být interní (pro firemní síť) nebo externí (pro koncová zařízení mimo síť). Externí zóna má vyplněnou DoH URL, na kterou se klientské aplikace zařízení připojují. Každá zóna obsahuje jeden kořenový subnet, od kterého se odvíjí celá hierarchie podsítí.

Podsítě

Podsíť je definovaná rozsahy IPv4 nebo IPv6 adres a může obsahovat libovolný počet dalších podsítí jako potomky. Strom podsítí umožňuje strukturovat firemní síť podle skutečné topologie. Na každou podsíť lze navázat jednu nebo více sad pravidel. Podsíť dědí nastavení sad pravidel svého předka, ovšem může být přepsáno.

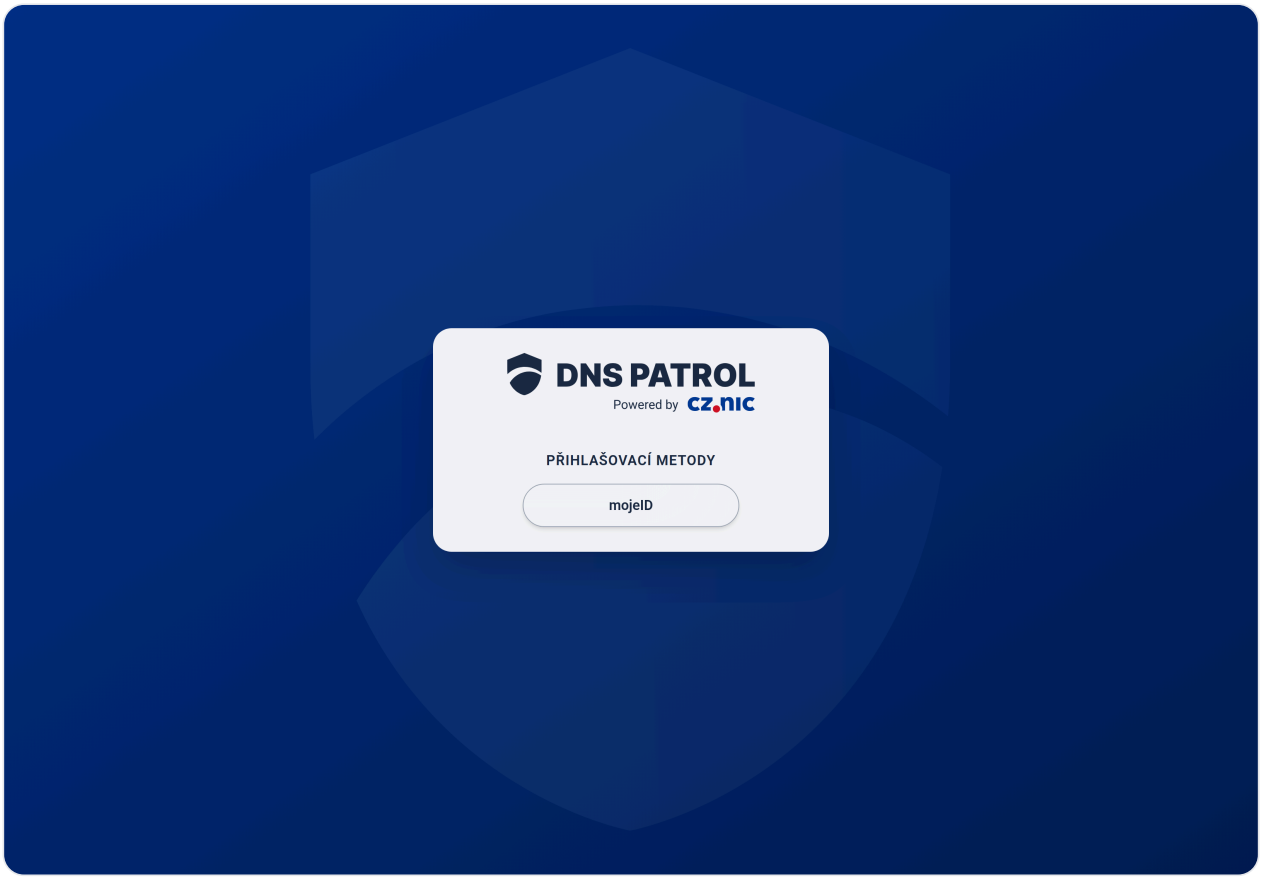
Sady pravidel

Sada pravidel je pojmenovaný seznam domén. Sada může být buď ve formě blokačního seznamu (blacklist), nebo seznamu výjimek (whitelist). Volitelně může mít přiřazený ML model pro vyhodnocování dotazů nad rámec statického seznamu.

Sada se na podsíť aplikuje s konkrétní akcí: `allow` (povolit), `block` (zablokovat) nebo `audit` (jen zaznamenat dotaz bez blokace). Výsledná konfigurace zóny se resolverům publikuje skrze Kafku.

Webový portál

Webový portál slouží pro nastavení chování systému DNS PATROL. Lze ho nalézt na adrese https://jezek.nic.cz/ ↗. Do administračního portálu je nutné se přihlásit použitím jedné z nabízených metod pro přihlášení, např. pomocí mojeID.



Obrázek 2 Přihlašovací stránka s nabízenými metodami přihlášení.

3.1 Navigační panel

Po přihlášení se k navigaci po aplikaci využívá postranní panel. V jeho horní části lze vidět jméno přihlášeného uživatele a jeho role, které určují, které sekce aplikace může procházet a měnit. Kromě navigačních odkazů do různých sekcí aplikace, které jsou detailněji popsány dále, obsahuje i tlačítko pro odhlášení uživatele.

Navigační panel lze zmenšit tlačítkem ‘Sbalit’ v jeho spodní části, či znovu rozbalit kliknutím na ikonku dvojité šipky.

O aplikaci

Stránka O aplikaci obsahuje licenční a další informace o aplikaci a systému DNS PATROL.

Co je nového

Obsahuje rychlý přehled změn aplikace pro každou vydanou verzi.

Odhlásit

Tlačítko pro odhlášení uživatele.

3.2 Práce s tabulkami

Následující chování je společné pro tabulky ve všech sekcích administračního portálu.

Viditelnost sloupců. Ikonou sloupců vedle názvu tabulky se otevře okno `Nastavení sloupců`. Zde lze zaškrtnutím sloupce zobrazit či skrýt, mezi sloupci vyhledávat podle názvu, tlačítkem `Resetovat` obnovit výchozí sadu a změny potvrdit tlačítkem `Uložit`. Nastavení se ukládá pro každého uživatele a tabulku zvlášť.

Šířka sloupců. Šířku sloupce lze změnit tažením za okraj v hlavičce tabulky. Dvojklikem na tentýž okraj se šířka daného sloupce vrátí na výchozí hodnotu.

Vymazání filtrů, řazení a šířek. Pokud je v tabulce aktivní filtr, řazení nebo vlastní šířka sloupců, objeví se nad tabulkou lišta s tlačítky `Vymazat všechny filtry`, `Vymazat řazení` a `Resetovat šířku sloupců`. Každé z nich se zobrazí jen tehdy, když je co vymazat.

Zachování filtrů. Ve výchozím stavu se filtry a řazení po opuštění stránky zahodí. Volbou `Uložit filtry tabulky` v sekci `Nastavení` lze zapnout jejich automatické obnovení při návratu na stránku.

Vyhledávání v nabídkách. Rozbalovací nabídky s výběrem polí a parametrů jsou řazené abecedně a obsahují vyhledávací pole. K zúžení seznamu stačí začít psát.

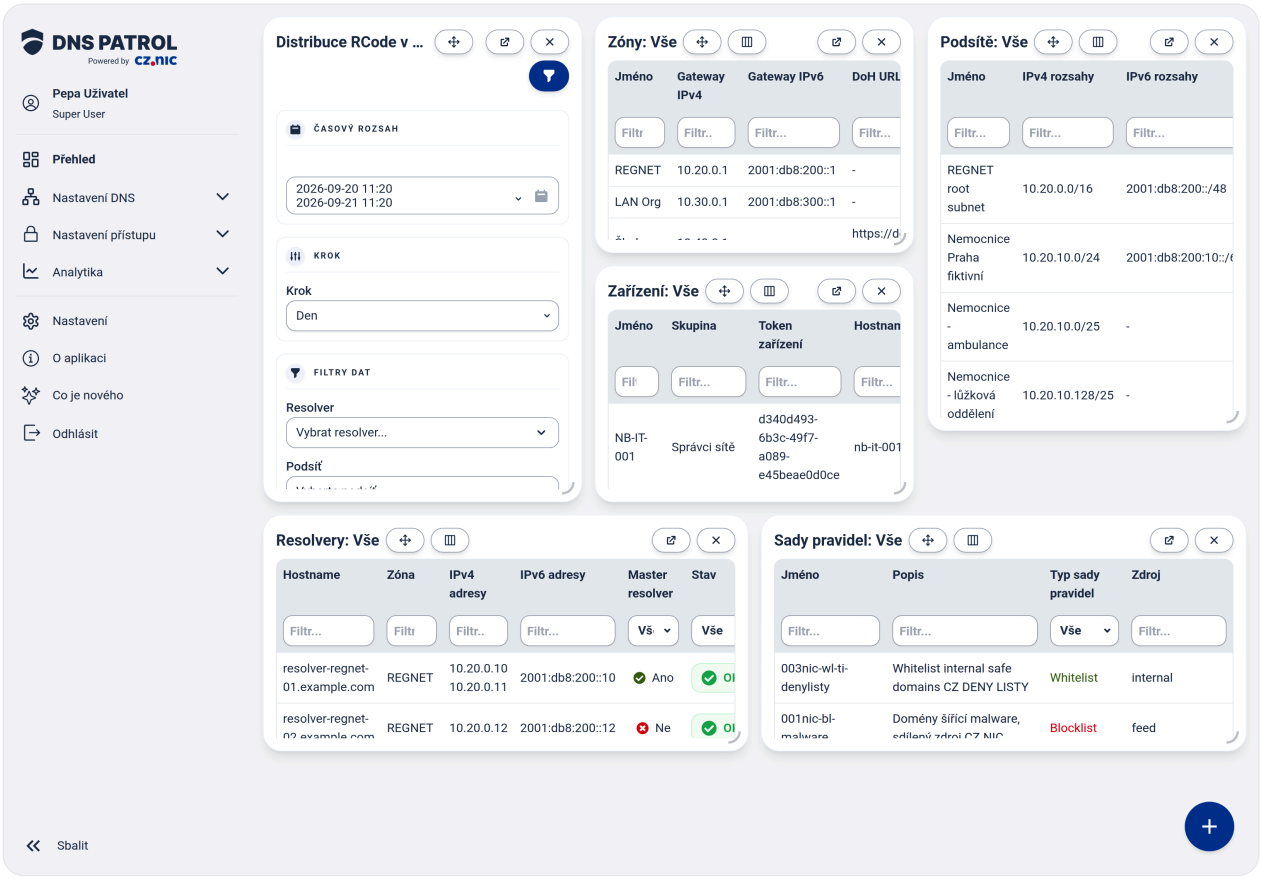
Oznámení novinek

Nové funkce se představují přímo na stránce, kde je lze použít. Okno s ukázkou lze přetáhnout stranou a funkci si rovnou vyzkoušet; mezi jednotlivými novinkami se listuje šipkami nebo kliknutím na tečku pod ukázkou. Zavřené okno se znovu otevře tlačítkem se žárovkou, které lze po obrazovce libovolně přesunout.

Přehled

V první sekci **Přehled** si přihlášený administrátor může sestavit vlastní Dashboard a přizpůsobit ho podle svých preferencí. Dashboard je tvořen widgety, které lze libovolně přidávat, přesouvat metodou drag-and-drop a měnit jejich velikost. Widgety se přidávají tlačítkem + v pravém dolním rohu Dashboardu, nebo z libovolné jiné stránky aplikace kliknutím na ikonu dashboardu u příslušné tabulky či grafu. Rozložení se ukládá pro každého uživatele zvlášť.

Widgety lze přesouvat tažením za horní okraj a měnit jejich velikost tažením za pravý dolní roh. Kliknutím na ikonku křížku v pravém horním rohu se widget odstraní; kliknutí na ikonku odkazu přesměruje na relevantní stránku v aplikaci.



Obrázek 3 Stránka Přehled s nastavenými widgety.

4.1 Přidání widgetu

Dostupné jsou widgety s přehledovými tabulkami zón, podsítí, resolverů, sad pravidel, uživatelů, zařízení a registračních kódů, stejně jako widgety s grafy a dlaždicemi ze stránky Statistiky.

Po kliknutí na ikonu **+** v pravém dolním rohu se zobrazí výběr z jednotlivých sekcí (Nastavení DNS, Nastavení přístupu a Analytika), dále z jednotlivých stránek a nakonec z konkrétních dlaždic na dané stránce. Po potvrzení výběru se widget přidá na Dashboard.

Alternativně lze widget přidat přímo z libovolné stránky aplikace kliknutím na ikonu dashboardu u příslušné tabulky či grafu.

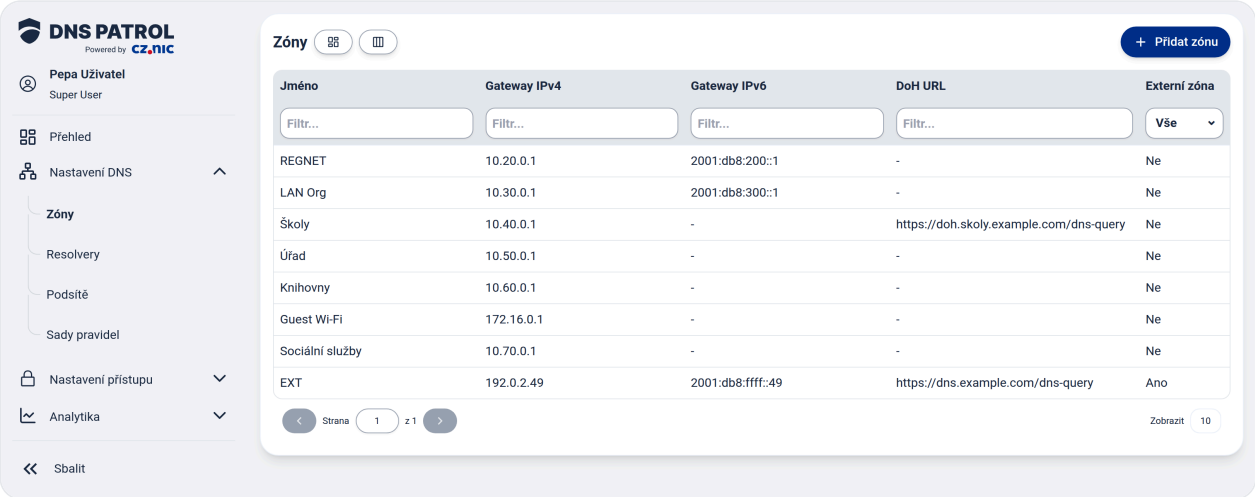
Nastavení DNS

Sekce nastavení DNS má několik podsekcí - Zóny, Resolvery, Podsítě, Sady Pravidel a Historie záznamů. Vše v této části administračního portálu se týká nastavení DNS pro použití společně s aplikací DNS PATROL.

5.1 Zóny

Zóna je logická síť, kterou portál potřebuje pro nastavení resolveru.

Po rozkliknutí záložky **Zóny** se zobrazí tabulka, ve které jsou všechny vytvořené zóny.



Obrázek 4 Tabulka zón.

Každá zóna obsahuje následující parametry:

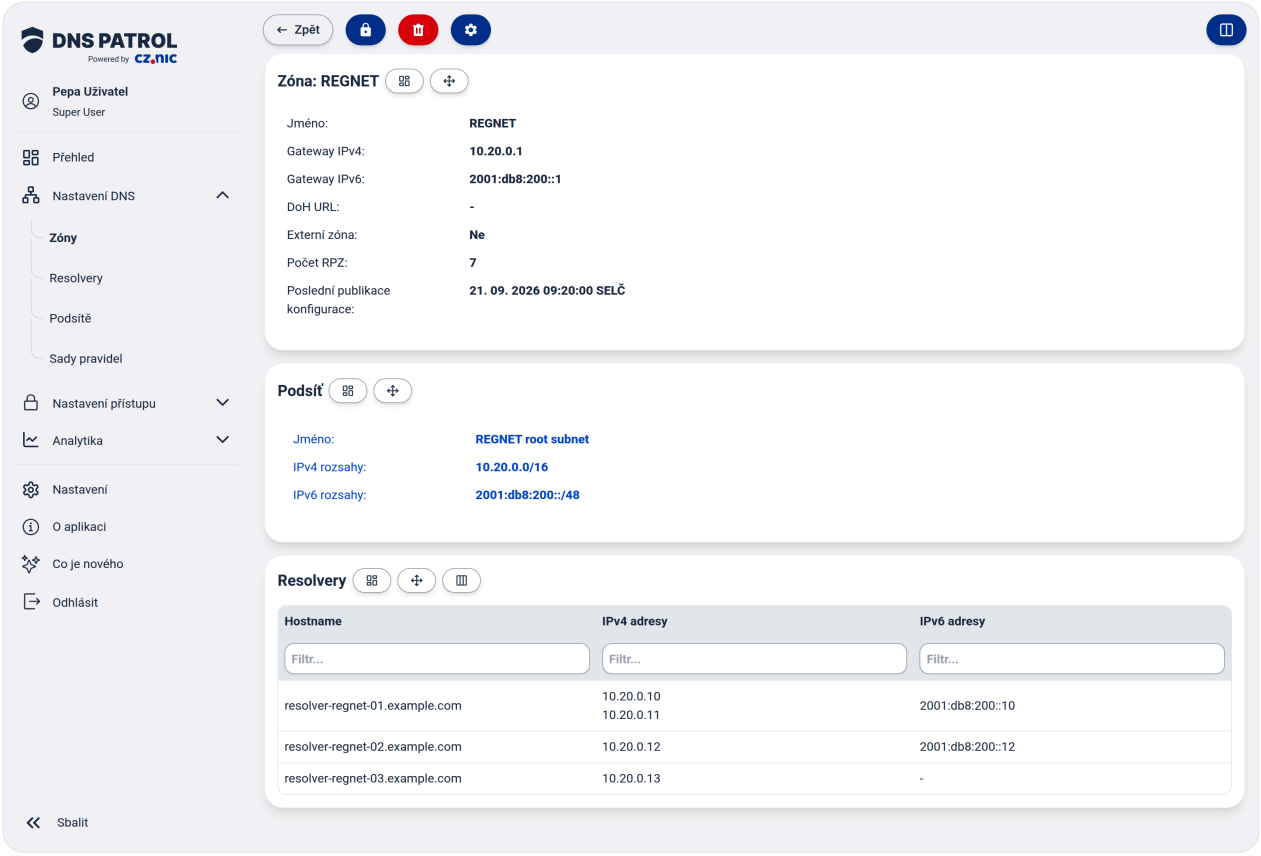
Položka	Popis
Jméno	Název zóny
Gateway IPv4	Zařízení (router) s IPv4 adresou, které slouží jako spojovací článek lokální sítí a vnějším světem
Gateway IPv6	Zařízení (router) s IPv6 adresou, které slouží jako spojovací článek lokální sítí a vnějším světem
DoH URL	Adresa serveru pro DNS over HTTPS
Externí zóna	Zda se jedná o externí zónu

Novou zónu lze vytvořit pomocí tlačítka **Přidat zónu** v pravém horním rohu administračního portálu. Následně je nutné vyplnit jednotlivé parametry a kliknout na tlačítko **Uložit**.

Po rozkliknutí jednotlivé zóny v tabulce se zobrazí její podrobnosti a je možné ji dále upravovat pomocí tlačítka s ozubeným kolečkem v pravém horním rohu obrazovky.

Kromě parametrů zadaných při vytvoření zóny jsou zde uvedeny **Počet RPZ** (kolik RPZ souborů se v zóně uplatní na základě sad pravidel použitých na jejích podsítích) a **Poslední publikace konfigurace** (kdy byla konfigurace zóny naposledy úspěšně publikována na resolvery).

Na této stránce dále nalezneme v části **Podsíť** konkrétní podsíť, ke které se daná zóna vztahuje. V části **Resolvery** najdeme tabulku s jednotlivými resolvery patřícími do dané zóny.

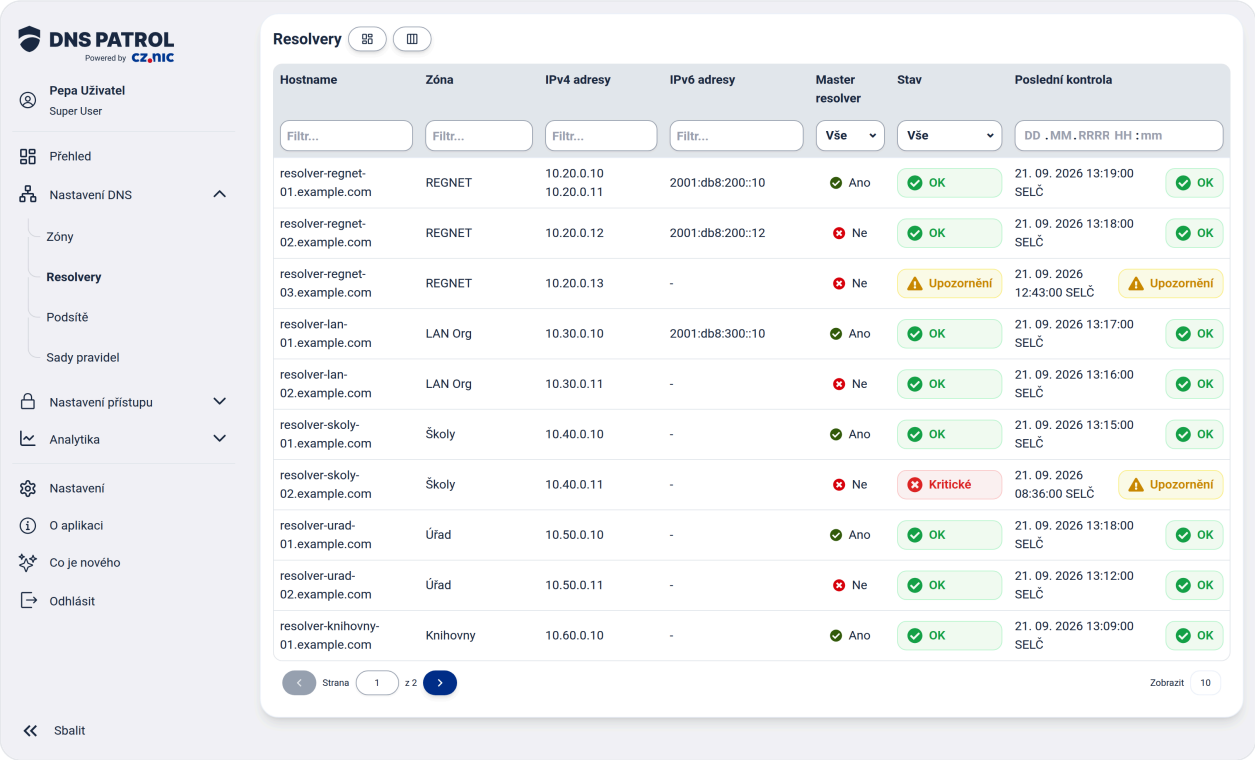


Obrázek 5 Podrobnosti zóny s navázanou podsítí a jejími resolvery.

5.2 Resolvery

Po rozkliknutí sekce **Resolvery** se zobrazí tabulka, ve které jsou všechny vytvořené resolvery.

Resolver je program, který odpovídá na DNS dotazy a určuje to, kam administrační portál nahrává konfigurační soubory.



Obrázek 6 Tabulka resolverů se stavem jednotlivých serverů.

Každý resolver obsahuje následující parametry:

Položka	Popis
Hostname	Jedinečné jméno přiřazené každému zařízení v síti
Zóna	V jaké zóně se resolver nachází
IPv4 adresy	IPv4 adresy jednotlivých zařízení v síti
IPv6 adresy	IPv6 adresy jednotlivých zařízení v síti
Master resolver	Zda se jedná o resolver, na který se dotazy posílají primárně
Stav	Stav resolveru - zda nevykazuje nějaké chyby
Poslední kontrola	Datum a čas, kdy byl resolver naposledy zkontrolován

Po rozkliknutí jednotlivého resolveru v tabulce se zobrazí jeho podrobnosti. V části Zóna je uvedeno, do které zóny resolver patří.

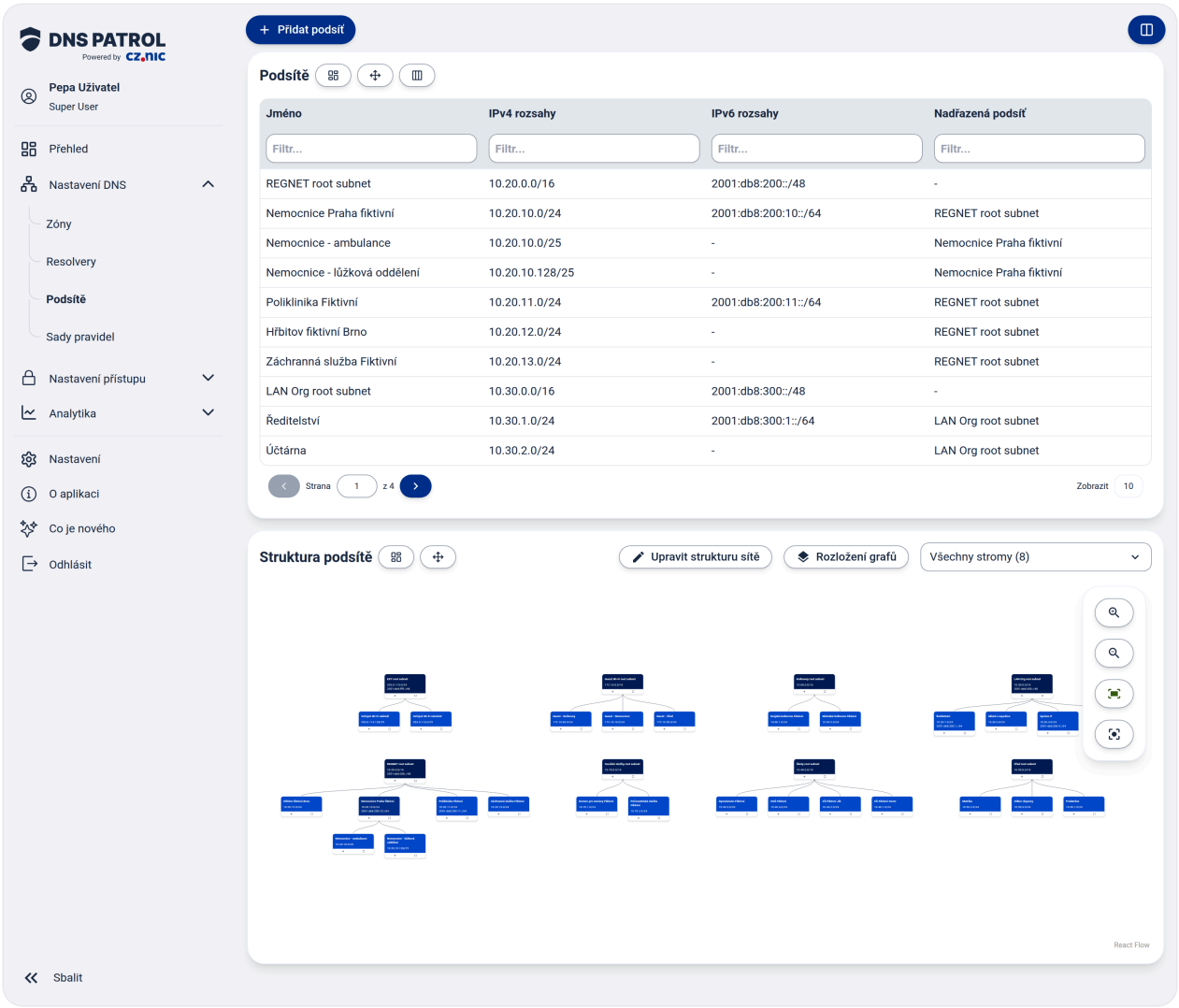
5.3 Podsítě

V sekci Podsítě najdeme v tabulce jednotlivé vytvořené nadřazené sítě a podřazené podsítě.

Každá podsíť obsahuje následující parametry:

Položka	Popis
Jméno	Název zóny
IPv4 rozsahy	Rozsahy IPv4 adres v této zóně
IPv6 rozsahy	Rozsahy IPv6 adres v této zóně
Nadřazená podsíť	Podsíť, která je dané síti nadřazena

Novou podsíť je možné vytvořit pomocí tlačítka **Přidat podsíť** v pravém horním rohu administračního portálu. Následně je nutné vyplnit jednotlivé parametry a kliknout na tlačítko **Uložit**. K jedné podsíti lze přidat více IPv4 i IPv6 rozsahů.



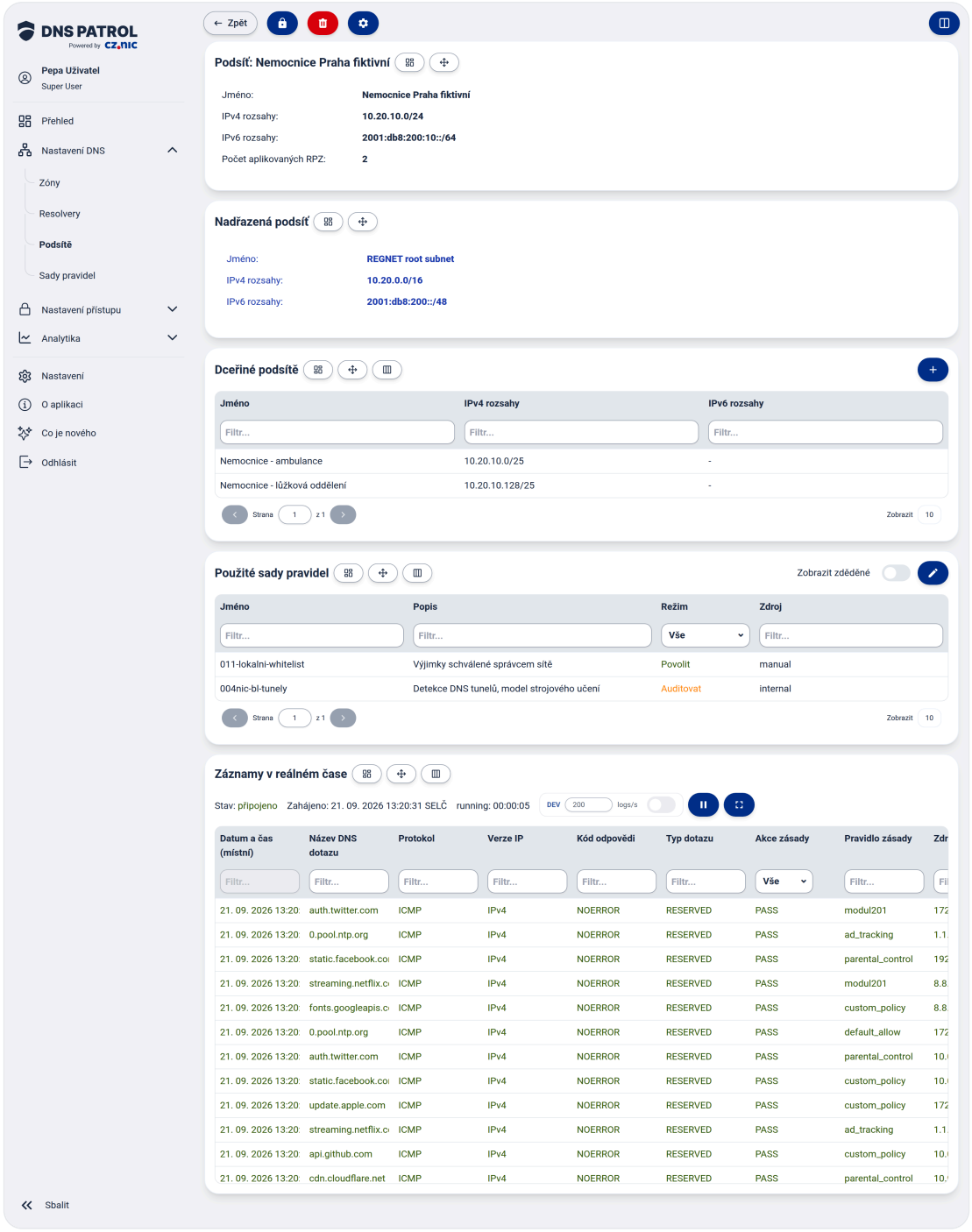
Obrázek 7 Tabulka podsítí a schéma jejich stromové struktury.

Pod tabulkou s podsítěmi najdeme grafickou strukturu jednotlivých sítí, kterou je možné upravovat pomocí tlačítka **Upravit strukturu sítě** v pravé části obrazovky. Dále je také možné pomocí tlačítka **Rozložení grafů** nastavit, jak se grafy budou zobrazovat. Do struktury sítě je možné přidat pomocí tlačítka **+** u dané podsítě další podsíť.

Po rozkliknutí podsítě v tabulce nebo v grafu se dostaneme na její detaily, které je možné dále upravovat. Zde nalezneme informace o podsíti, mezi nimi i **Počet aplikovaných RPZ** (kolik RPZ souborů se uplatní na tuto podsíť a její dceřiné podsítě), dále informace o nadřazené podsíti a také seznam dceřiných podsítí. Dále zde také najdeme tabulku použitých sad pravidel, které lze síti přiřadit pomocí tlačítka se symbolem propisky v pravé části obrazovky nad tabulkou. Ze seznamu pravidel vybereme, který chceme použít, a jeho stav nastavíme pomocí přepínače:

- **Enable**: sada pravidel je na podsíť aplikována, domény ze seznamu jsou blokovány, nebo povoleny, podle typu sady pravidel (Blocklist nebo Whitelist)
- **Audit**: domény ze sady pravidel jsou pouze sledovány a zapisovány do logu, bez blokování či povolování
- **Disable**: sada pravidel není na podsíť aplikována
- Následně klikneme na `Uložit`.

Rozkliknutá podsíť také obsahuje část `Záznamy v reálném čase`, kde je možné sledovat, co bylo blokováno a také lze kontrolovat přístupy k doménám z použité sady pravidel nastavené jako `Auditovat`.



Obrázek 8 Podrobnosti podsítě s dceřinými podsítěmi, použitými sadami pravidel a záznamy v reálném čase.

Real-time logy

Příklad interpretace informací v logu.

Kód odpovědi	Akce zásady	Pravidlo zásady	Význam
NXDOMAIN	-	-	doména není dostupná
NXDOMAIN	BLOCK	-	doména je blokována resolverem na základě vnitřních pravidel resolveru
NXDOMAIN	BLOCK	modul201	doména je blokována resolverem na základě zadaného Pravidla zásad `modul201` nastaveného na `Blokování`

5.4 Sady pravidel

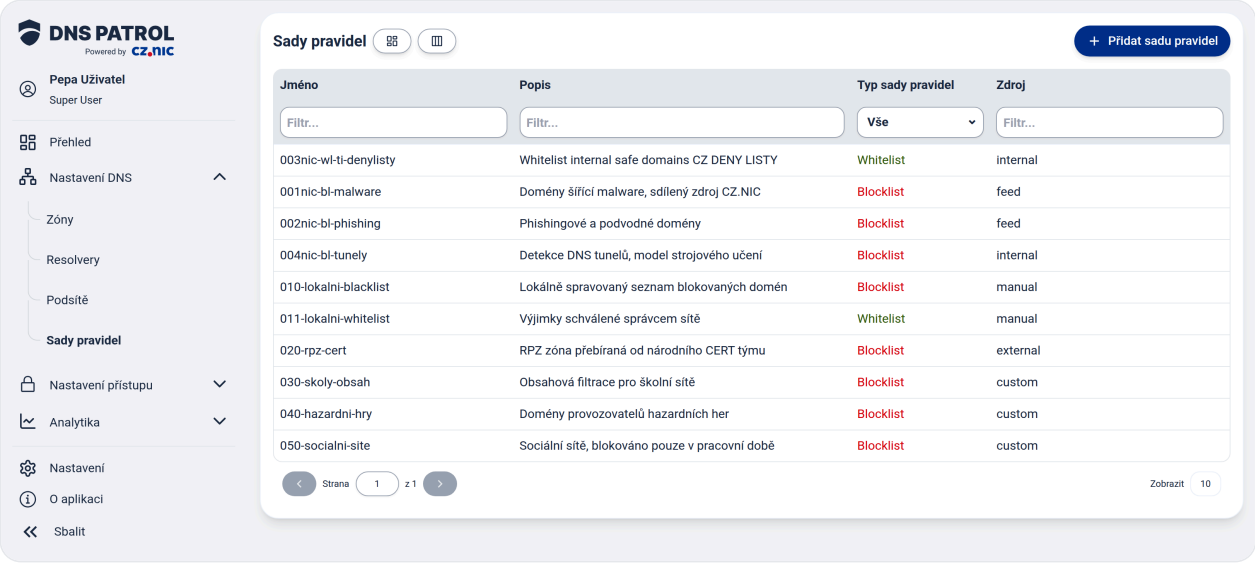
Sady pravidel obsahují jednotlivé sady pravidel se seznamy domén, které pak mohou být použity jako:

- **Blocklist**: seznam těchto domén bude blokován (barva červená)
- **Whitelist**: seznam těchto domén je povolen (barva zelená)

Každá sada pravidel obsahuje následující parametry:

Položka	Popis
Jméno	Název sady pravidel
Popis	Pro co se seznam domén s tímto pravidlem používá
Domény	Seznam domén, na které se vztahuje dané pravidlo
Typ sady pravidel	Zda je sada pravidel Blocklist, nebo Whitelist

Novou sadu pravidel lze vytvořit pomocí tlačítka `Přidat sadu pravidel` v pravém horním rohu administračního portálu. Následně je nutné vyplnit jednotlivé parametry a kliknout na tlačítko `Uložit`. Jméno sady pravidel musí být pouze alfanumerické s pomlčkami, bez mezer a dalších speciálních znaků a alespoň dva znaky dlouhé.

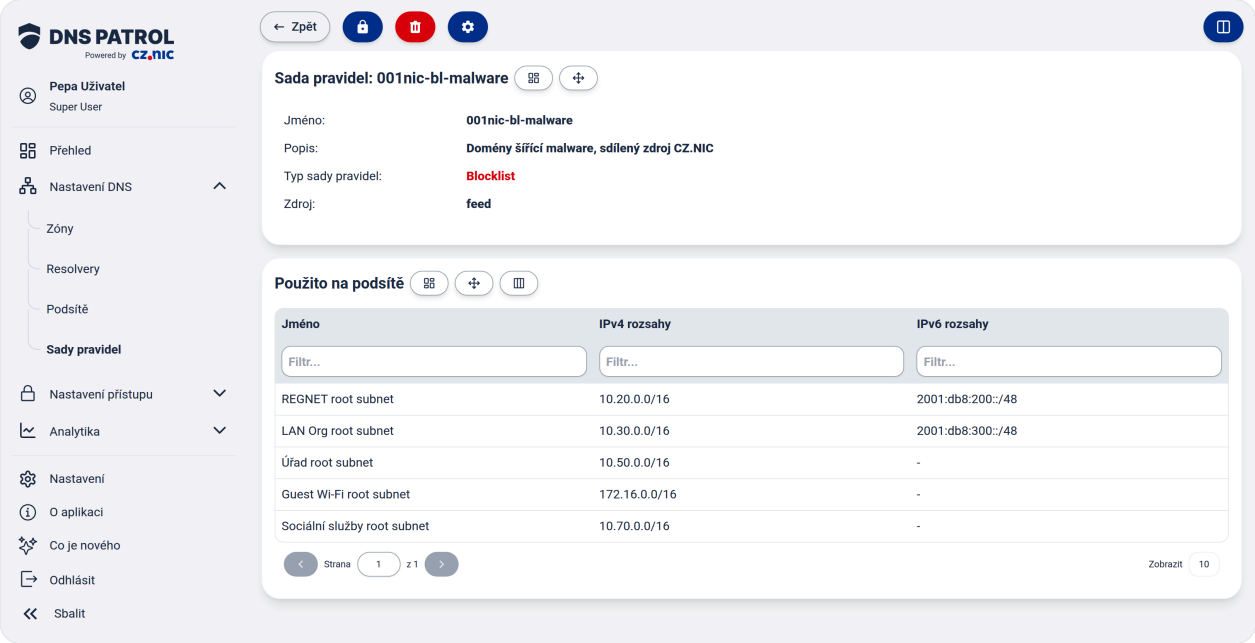


Obrázek 9 Tabulka sad pravidel.

Po rozkliknutí sady pravidel v tabulce se zobrazí další informace o dané sadě pravidel.

Dále zde vidíme `Filtrované domény` - tedy seznam domén, na které se daná sada pravidel vztahuje. Pomocí tlačítka ‘Rozšířit z CSV’ lze nahrát soubor domén, kterými je seznam domén rozšířen. Stisknutí tlačítka ‘Nahradit z CSV’ nahradí všechny domény v této sadě doménami z nahraného souboru. Tlačítkem ‘Exportovat do CSV’ lze stáhnout seznam domén do CSV souboru.

V části **Použito na podsítě** zjistíme, pro které podsítě byla tato sada pravidel použita.



Obrázek 10 Podrobnosti sady pravidel s filtrovanými doménami.

Na této stránce je také možné sadu pravidel dále měnit a upravovat - pomocí tlačítka s ozubeným kolečkem v pravém horním rohu administračního portálu. Případně lze sadu pravidel smazat pomocí červeného tlačítka s ikonou popelnice.

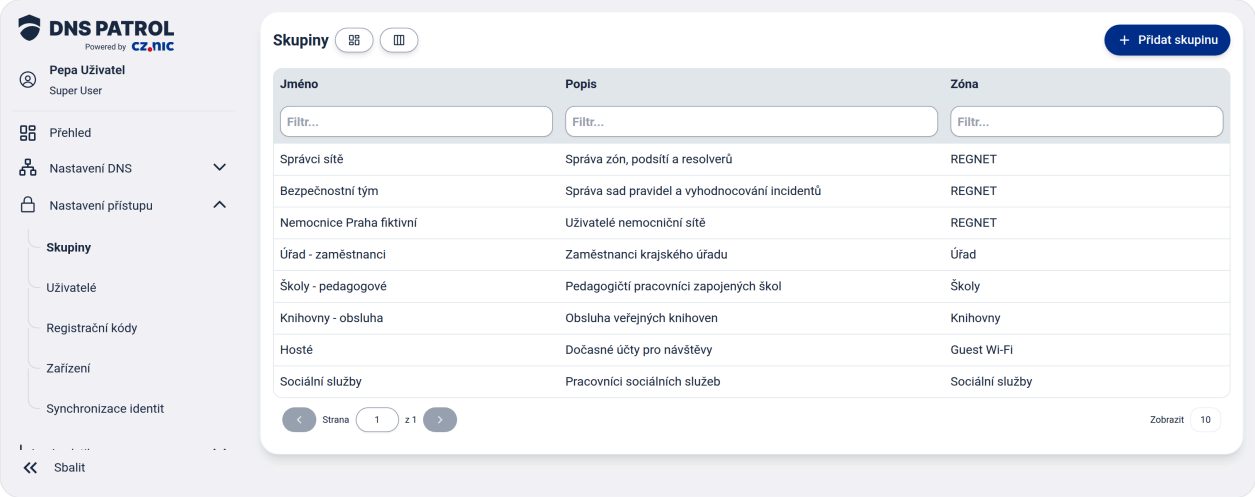
Řazení: Pro lepší přehlednost lze sady pravidel seřadit podle sloupce kliknutím na hlavičku sloupce. Stejně to funguje ve všech dalších tabulkách na všech sloupcích.

Nastavení přístupu

V této sekci se pracuje s nastavením pro jednotlivé uživatele - přiřazení jejich práv, rozdělení do skupin a tvorba kódu zařízení.

6.1 Skupiny

Skupiny jsou logickou strukturou pro třídění uživatelů.



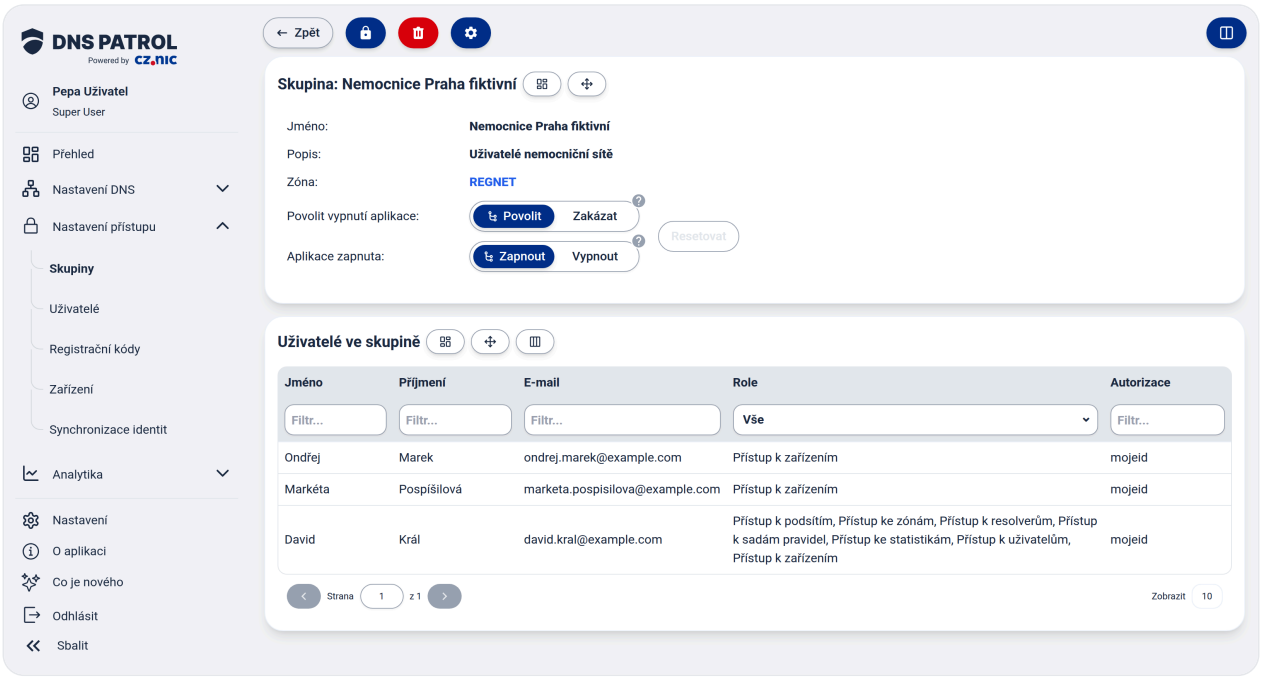
Obrázek 11 Tabulka skupin.

Skupiny obsahují následující parametry:

Položka	Popis
Jméno	Název skupiny
Popis	Popis skupiny
Zóna	Pod kterou zónu skupina patří

Po rozkliknutí skupiny je možné skupinu upravovat (tlačítko ozubeného kolečka v pravém horním rohu), nebo smazat (červené tlačítko popelnice v pravém horním rohu).

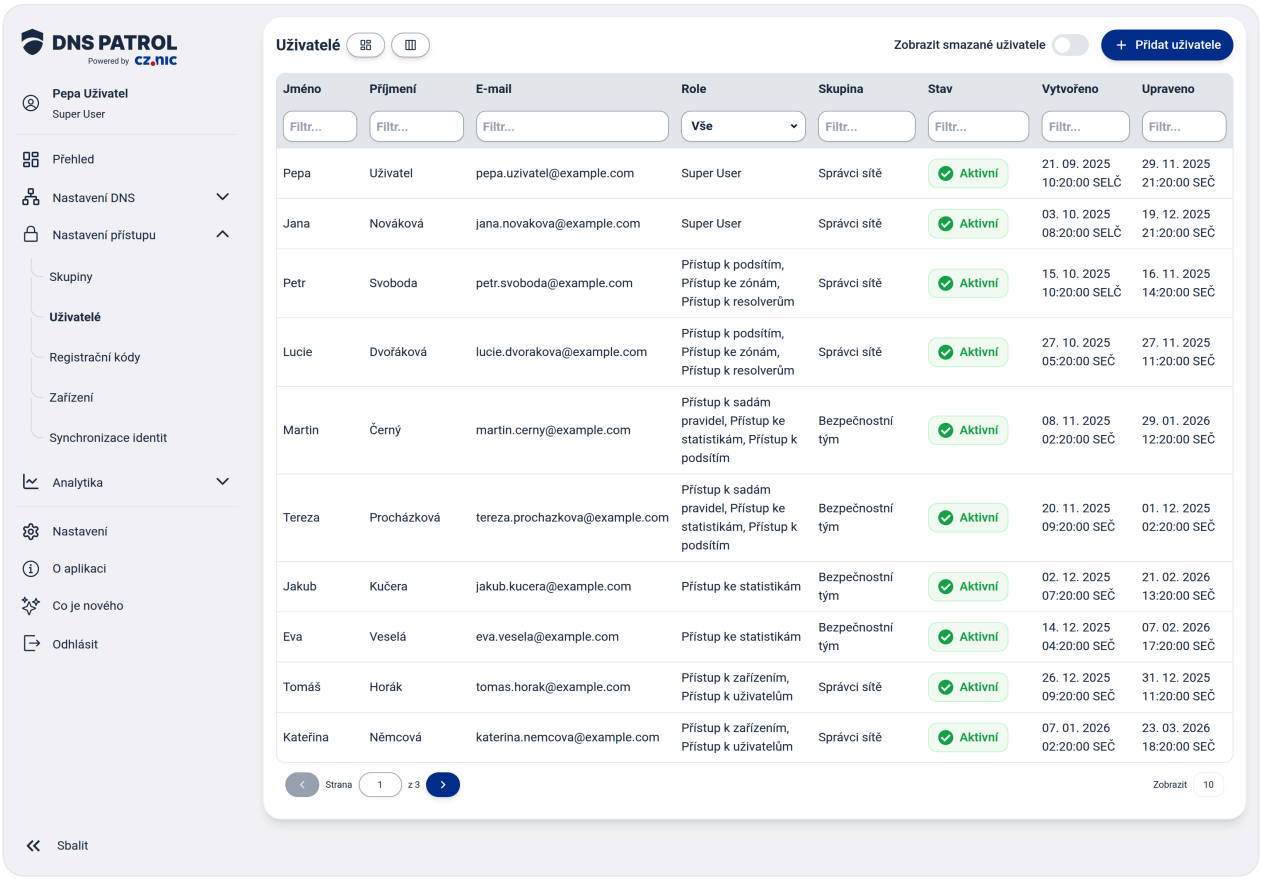
Novou skupinu lze vytvořit pomocí tlačítka **Přidat skupinu** v pravém horním rohu administračního portálu. Následně je nutné vyplnit jednotlivé parametry a kliknout na tlačítko **Uložit**.



Obrázek 12 Podrobnosti skupiny se seznamem jejích uživatelů.

6.2 Uživatelé

Tato podsekce obsahuje seznam uživatelů.



Obrázek 13 Tabulka uživatelů s přiřazenými rolemi a skupinami.

Každý uživatel má následující parametry:

Položka	Popis
Jméno	Jméno uživatele
Příjmení	Příjmení uživatele
E-mail	Emailová adresa uživatele
Role	Role uživatele (Super uživatel, přístup k vybraným částem WA, bez přístupu)
Skupina	Do jaké skupiny uživatel patří
Vytvořeno	Kdy byl uživatel založen
Aktualizováno	Kdy byl uživatel naposledy upraven

Nového uživatele lze vytvořit pomocí tlačítka **Přidat uživatele** v pravém horním rohu administračního portálu. Následně je nutné vyplnit jednotlivé parametry a kliknout na tlačítko **Uložit**.

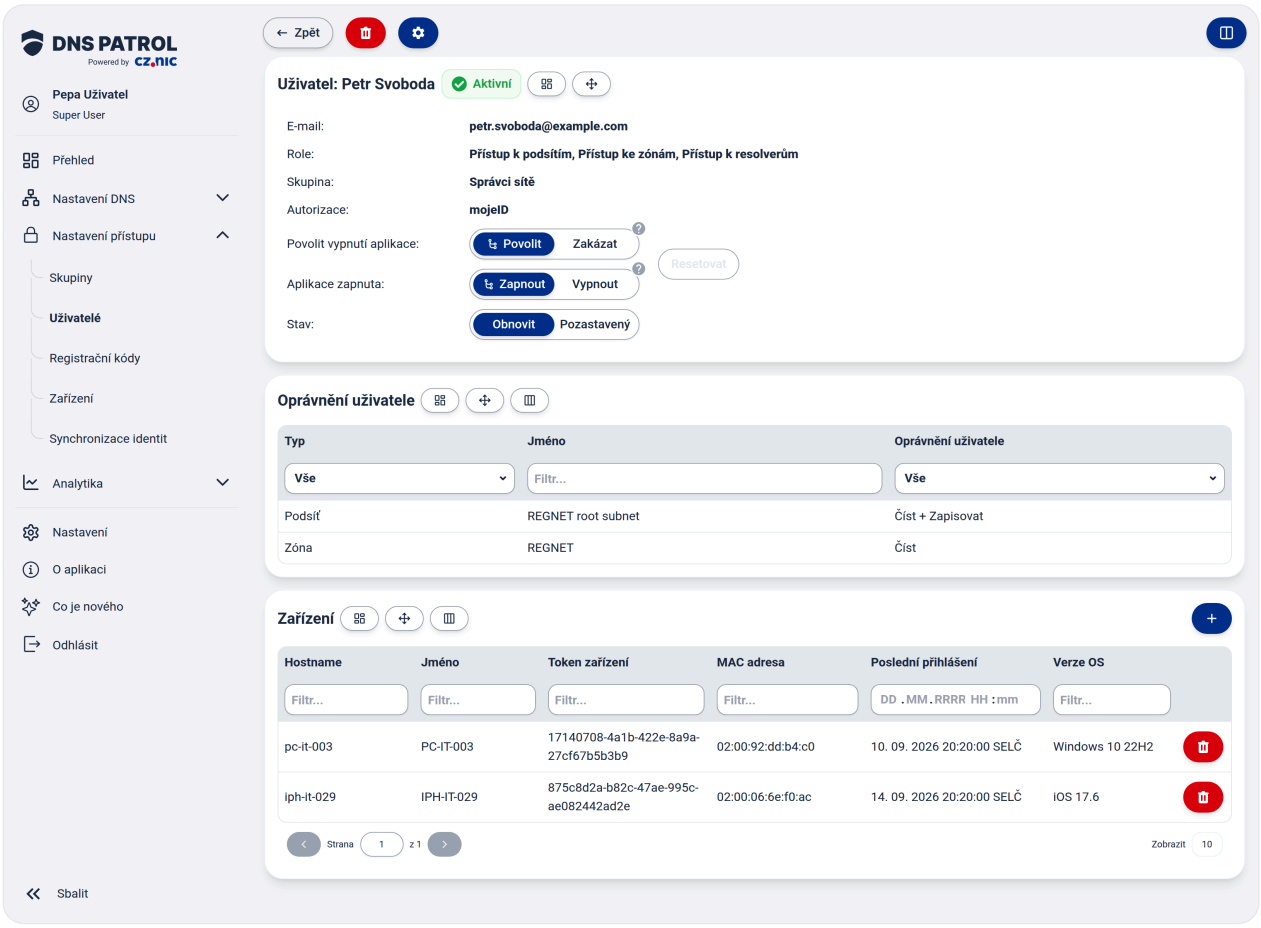
Po rozkliknutí daného uživatele se zobrazí informace o uživateli. Uživatele je možné upravovat po kliknutí na tlačítko s ozubeným kolečkem v pravé horní části administračního portálu, nebo ho smazat po kliknutí na červené tlačítko s ikonou popelnice.

V části **Zařízení** je seznam zařízení, které uživatel používá. Zde je možné přidat nové zařízení, resp. vygenerovat unikátní klíč (registrační kód), kterým se uživatel přihlašuje do aplikace DNS PATROL pomocí tlačítka **+** v pravé části administračního portálu nad tabulkou **Zařízení**. Následně je potřeba vyplnit jednotlivé položky - předpona (prefix, který se dá před název zařízeni), limit použití (na kolik zařízení smí být kód použit) a **Vyprší dne** (platnost kódu ve dnech) a kliknout na tlačítko **Uložit**.

Jednotlivá zařízení pak obsahují následující parametry:

Položka	Popis
Hostname	Jedinečné jméno přiřazené každému zařízení v síti, nahrazuje číselné IP adresy
Jméno	Název zařízení
Token zařízení	Identifikátor zařízení
MAC adresa	MAC adresa zařízení
Poslední přihlášení	Kdy se zařízení naposledy přihlásilo k síti

V tabulce je u každého zařízení červené tlačítko s ikonou popelnice, které je možné použít pro smazání zařízení.



Obrázek 14 Podrobnosti uživatele se seznamem jeho zařízení.

Pozvánka uživatele

Uživateli, který zatím nemá připojený žádný způsob přihlášení, lze vygenerovat pozvánku. Tlačítkem s ikonou přidání uživatele v pravé horní části stránky se otevře okno **Pozvat uživatele**, kde se tlačítkem **Vygenerovat odkaz** vytvoří odkaz s omezenou platností. Odkaz je jednorázový, vygenerováním nového se předchozí zneplatní.

Po otevření odkazu se pozvanému zobrazí uvítací stránka, na které si k účtu připojí svého poskytovatele přihlášení. Zda už pozvánku přijal, je vidět na detailu uživatele v položce **Autorizace**.

Vypnutí aplikace

Na detailu uživatele a na detailu skupiny se nastavuje, jak se má aplikace DNS PATROL na zařízeních chovat:

Položka	Popis
Povolit vypnutí aplikace	**Povolit** / **Zakázat** – zda uživatel smí aplikaci sám vypnout
Aplikace zapnuta	**Zapnout** / **Vypnout** – zda je aplikace zapnutá

Hodnoty se dědí: uživatel přebírá nastavení své skupiny, skupina přebírá výchozí nastavení systému. Zděděná hodnota je označena ikonou u vybrané možnosti, výběrem jiné možnosti se pro daného uživatele či skupinu přepíše. Tlačítkem **Resetovat** se obě položky vrátí zpět k dědění.

Role uživatele

Role uživatele se dají vybrat jednotlivě nebo více rolí najednou. Jednotlivé přístupy se slučují.

Role uživatele	ID role	Zobrazené sekce ve WA
Super User	super_user	přístup ke všem sekcím Administračního portálu
Přístup k podsítím	subnets_viewer	přístup do sekce Podsítě
Přístup ke zónám	zones_viewer	přístup do sekce Zóny
Přístup k resolverům	resolvers_viewer	přístup do sekce Resolvery
Přístup k sadám pravidel	rulesets_viewer	přístup do sekce Sady pravidel
Přístup ke statistikám	statistics_viewer	přístup do sekce Analytika: Statistiky, Historie záznamů, Pasivní DNS, Soubory
Přístup k uživatelům	users_viewer	přístup do sekcí Skupiny a Uživatelé
Přístup k zařízením	devices_viewer	přístup do sekcí Registrační kódy a Zařízení
Bez přístupu ke správě DNS	no_role	přístup pouze do sekce Přehled

Nastavení přístupu ke čtení, zápisu a mazání se nastavuje takto: `Nastavení přístupu` > `Skupiny` > kliknu na skupinu, kterou chci editovat > zobrazí se informace o Skupině a seznam uživatelů > kliknutím na ikonu zámečku vpravo nahoře se otevře dialogové okno se všemi uživately > pro každého uživatele mohu zvolit jednu ze tří možností > uložím tlačítkem `Uložit`.

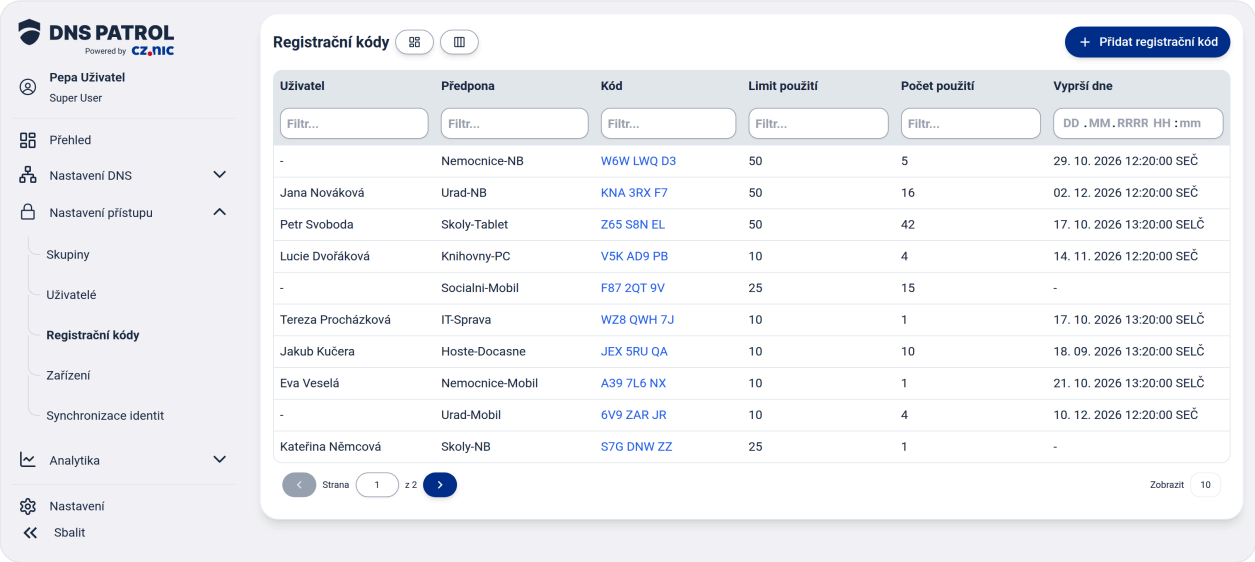
6.3 Registrační kódy

V této podsekci jsou uvedené jednotlivé registrační kódy, které se používají při registraci daného zařízení po prvním spuštění aplikace DNS PATROL.

Jednotlivé registrační kódy pak obsahují následující parametry:

Položka	Popis
Jméno	Jméno uživatele
Příjmení	Příjmení uživatele
Předpona	Prefix, který je před názvem zařízení
Kód	Registrační kód pro aplikaci DNS PATROL
Limit použití	Na kolika zařízeních smí být kód použit
Počet použití	Na kolika zařízeních byl kód použit
Vyprší dne	Kdy kód přestane být platný

Nový registrační kód je možné vytvořit pomocí tlačítka `Přidat registrační kód` v pravém horním rohu administračního portálu. Následně je nutné vyplnit jednotlivé parametry a kliknout na tlačítko `Uložit`.



Obrázek 15 Tabulka registračních kódů.

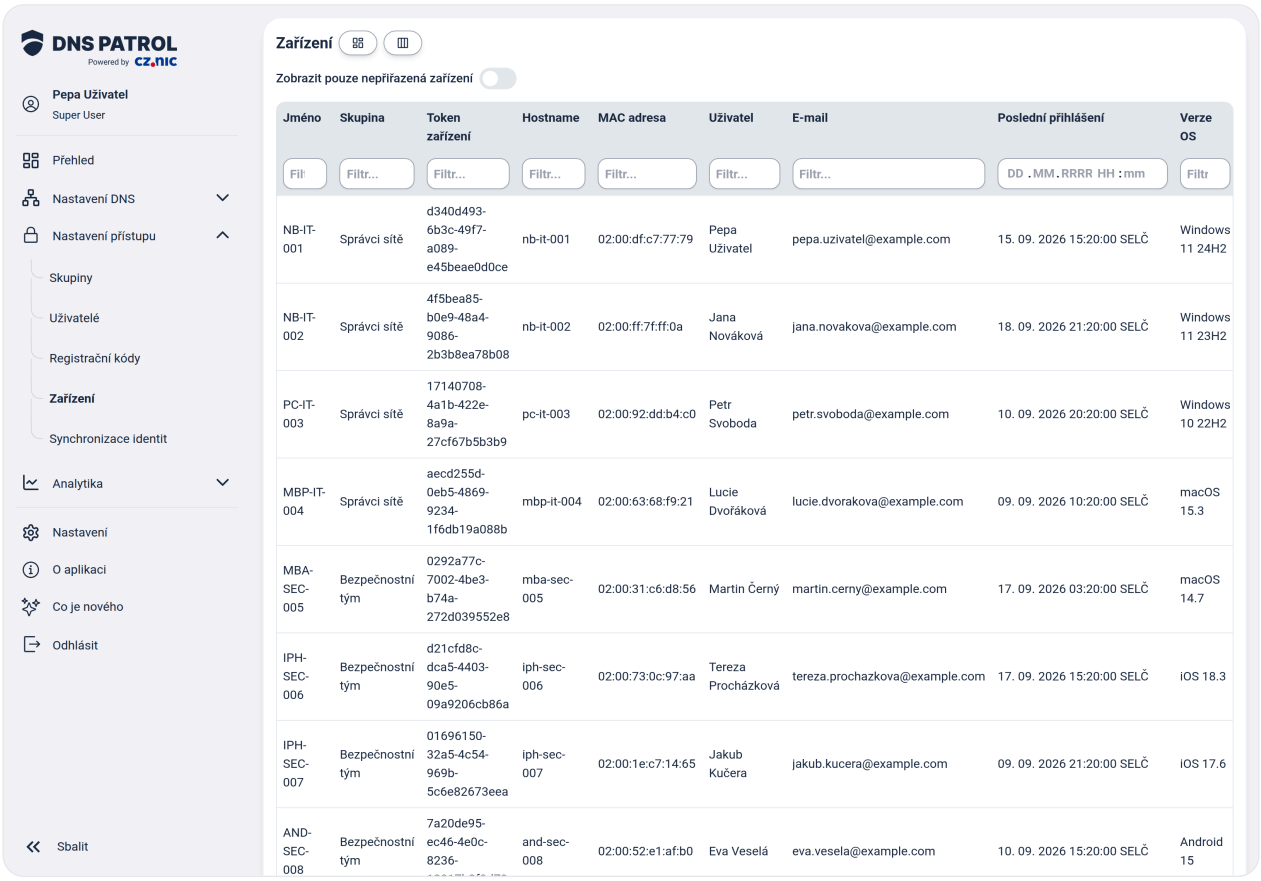
6.4 Zařízení

Tato podsekce obsahuje seznam všech registrovaných zařízení s možností zobrazit pouze ty, co nejsou přiřazeny k žádnému uživateli.

Jednotlivé zařízení obsahují tyto parametry:

Položka	Popis
Jméno	Jméno zařízení (obsahující prefix z registračního kódu)
Hostname	Systémové jméno zařízení
MAC adresa	MAC adresa zařízení
Uživatel	Jméno uživatele (nebo tlačítko s možností uživatele přiřadit)
E-mail	E-mail uživatele
Poslední přihlášení	Kdy se zařízení naposledy přihlásilo do systému

Nový kód zařízení lze vytvořit pomocí tlačítka „Přidat kód zařízení“ v pravém horním rohu administračního portálu. Poté vyplňte parametry a klikněte na „Uložit“.



Obrázek 16 Tabulka zařízení.

6.5 Synchronizace identit

Tato podsekce je přístupná pouze roli Super User a slouží ke sledování automatického přebírání uživatelů z externích zdrojů identit.

Zdroje identit

Tabulka **Zdroje identit** obsahuje nakonfigurované zdroje a jejich aktuální stav:

Položka	Popis
Jméno	Název zdroje
Typ	Typ zdroje
Stav	Zda je zdroj aktivní, nebo neaktivní
Průběh synchronizace	Zda právě probíhá synchronizace, nebo je zdroj nečinný
Interval synchronizace	Jak často se zdroj synchronizuje
Další spuštění	Za jak dlouho proběhne další synchronizace
Poslední spuštění	Výsledek posledního běhu spolu s počtem vytvořených a aktualizovaných uživatelů a časem dokončení

Tlačítkem **Synchronizovat** v posledním sloupci lze u aktivního zdroje spustit synchronizaci ručně, bez čekání na další naplánované spuštění.

Historie synchronizací

Tabulka **Historie synchronizací** obsahuje jednotlivé běhy. Rozbalovací nabídkou nad tabulkou lze zobrazit pouze běhy vybraného zdroje.

Položka	Popis
Stav	Zda běh skončil úspěchem, nebo chybou
Spouštěč	Zda šlo o plánovaný, nebo manuálně spuštěný běh
Čas zahájení	Kdy běh začal
Čas dokončení	Kdy běh skončil
Vytvoření uživatelé	Počet nově založených uživatelů
Aktualizovaní uživatelé	Počet změněných uživatelů
Deaktivovaní uživatelé	Počet uživatelů deaktivovaných na základě zdroje
Chybná data	Počet záznamů, které se nepodařilo zpracovat
Přeskočeno	Počet logicky smazaných a manuálně založených uživatelů, kterých se synchronizace nedotkla
Sloučené běhy	Kolik shodných po sobě jdoucích běhů je v řádku sloučeno
Chyba	Chybová hláška, pokud běh selhal

Po rozkliknutí řádku se otevře okno **Podrobnosti synchronizace** se souhrnem běhu (stav, spouštěč, doba trvání) a se seznamy konkrétních dotčených záznamů - vytvoření a aktualizovaní uživatelé, deaktivovaní a přeskočení uživatelé, vytvořené skupiny uživatelů a chybná data i s důvodem selhání.

Analytika

Tato kategorie obsahuje různé statistiky z resolverů, pasivního DNS a dat z Cesnet Warden.

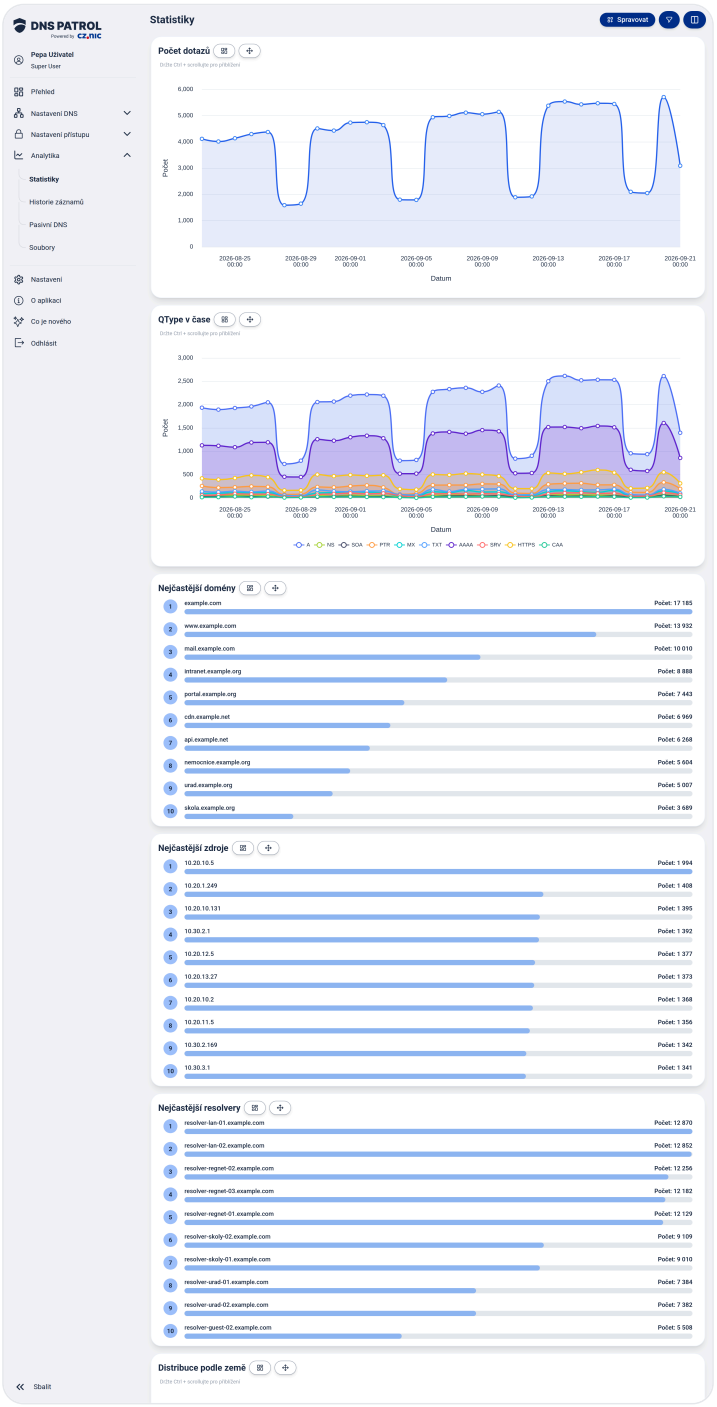
7.1 Statistiky

V této sekci můžete prohlížet statistiky a grafy související s chodem aplikace.

Parametry zobrazovaných grafů (Krok (Den, Hodina, Minuta), časové rozmezí (Od data – Do data), Resolver, Doména, IP, Země) nastavíte v horní části stránky. Filtry můžete zobrazit nebo skrýt kliknutím na příslušný nápis „Zobrazit filtry“ či „Skrýt filtry“ vedle názvu sekce Statistiky.

- **Počet dotazů** - Vývoj počtu DNS dotazů, které aplikace zpracovala.
- **QType v čase** - Vývoj počtu DNS dotazů rozlišitelný podle jejich typu (např. A, NS, SOA atd.). Viditelnost jednotlivých typů můžete zapínat nebo vypínat kliknutím na jejich název v legendě v pravé části grafu.
- **Nejčastější domény** - Žebříček domén seřazený podle četnosti, s jakou je aplikace zpracovala. Pro každou doménu je uveden celkový počet dotazů.
- **Nejčastější zdroje** - Žebříček zdrojových IP adres seřazený podle četnosti, s jakou generovaly DNS dotazy. Pro každou IP adresu je uveden celkový počet dotazů.
- **Nejčastější servery** - Žebříček resolverů/serverů seřazený podle celkového počtu DNS dotazů, které zpracovaly. Zobrazuje, které nesly největší zátěž.
- **Distribuce podle země** - Teplotní mapa světa znázorňující geografické rozložení DNS dotazů. Intenzita barvy odpovídá celkovému počtu dotazů pocházejících z dané země. Přesná hodnota pro konkrétní zemi se zobrazí po najetí kurzorem myši na danou oblast.
- **Matice QType a RCode** - Zobrazení distribuce typů DNS dotazů (QType) podle návratových kódů (RCode), které dotazy obdržely po zpracování. Graf slouží k vizuálnímu posouzení, zda se dané typy dotazů (např. A, AAAA, MX, atd.) vrací s očekávaným výsledkem (NOERROR) nebo se setkávají s chybami, jako jsou SERVFAIL (selhání serveru), NXDOMAIN (doména neexistuje), REFUSED (dotaz odmítnut) či NOTIMP (požadovaná funkce není podporována). Počet dotazů jednotlivých typů v rámci daného RCode se zobrazí po najetí kurzorem myši na příslušný sloupec. Viditelnost QType v grafu můžete zapínat nebo vypínat kliknutím na jeho název v legendě v pravé části grafu.
- **Distribuce RCode v čase** - Graf vizualizuje souběžný vývoj četnosti jednotlivých návratových kódů. Viditelnost jednotlivých typů návratových kódů v grafu můžete zapínat nebo vypínat kliknutím na jejich název v legendě v pravé části grafu.
- **Akce zásad** - Koláčový graf znázorňující celkové rozdělení DNS dotazů podle akce, kterou na ně aplikovaly nastavené sady pravidel. Graf slouží k posouzení, jaký podíl dotazů je PASS (povolen), BLOCK (blokován) či AUDIT (povolen a sledován). Přesné číselné hodnoty se zobrazí po najetí kurzorem myši na příslušnou část.
- **Akce zásad podle pravidla** - Skládaný sloupcový graf zobrazující, které konkrétní sady pravidel se podílejí na výsledné akci s dotazem (PASS, BLOCK, AUDIT). Graf slouží k vizuálnímu posouzení efektivity a zapojení jednotlivých pravidel. Viditelnost jednotlivých pravidel v grafu můžete zapínat nebo vypínat kliknutím na jejich název v legendě umístěné v pravé části grafu. Přesný počet dotazů pro konkrétní pravidla v rámci dané akce se zobrazí po najetí kurzorem myši na příslušný sloupec.
- **Distribuce QType** - Koláčový graf znázorňující celkové rozdělení DNS dotazů podle jejich typu. Přesné číselné hodnoty se zobrazí po najetí kurzorem myši na příslušnou část.

- **QPS podle serveru** - Vizualizace souběžného vývoje zátěže jednotlivých resolverů/serverů měřené v Dotazech za sekundu (QPS). Viditelnost jednotlivých serverů v grafu můžete zapínat nebo vypínat kliknutím na jejich název v legendě.
- **NXDomain v čase** - Vývoj počtu dotazů končících chybou NXDOMAIN (doména neexistuje).
- **ServFail v čase** - Vývoj počtu dotazů končících chybou SERVFAIL (selhání serveru/neúspěšné zpracování).
- **Doména v sadách pravidel** - Zobrazí, v jakých sadách pravidel se nachází doména zadaná ve filtru.

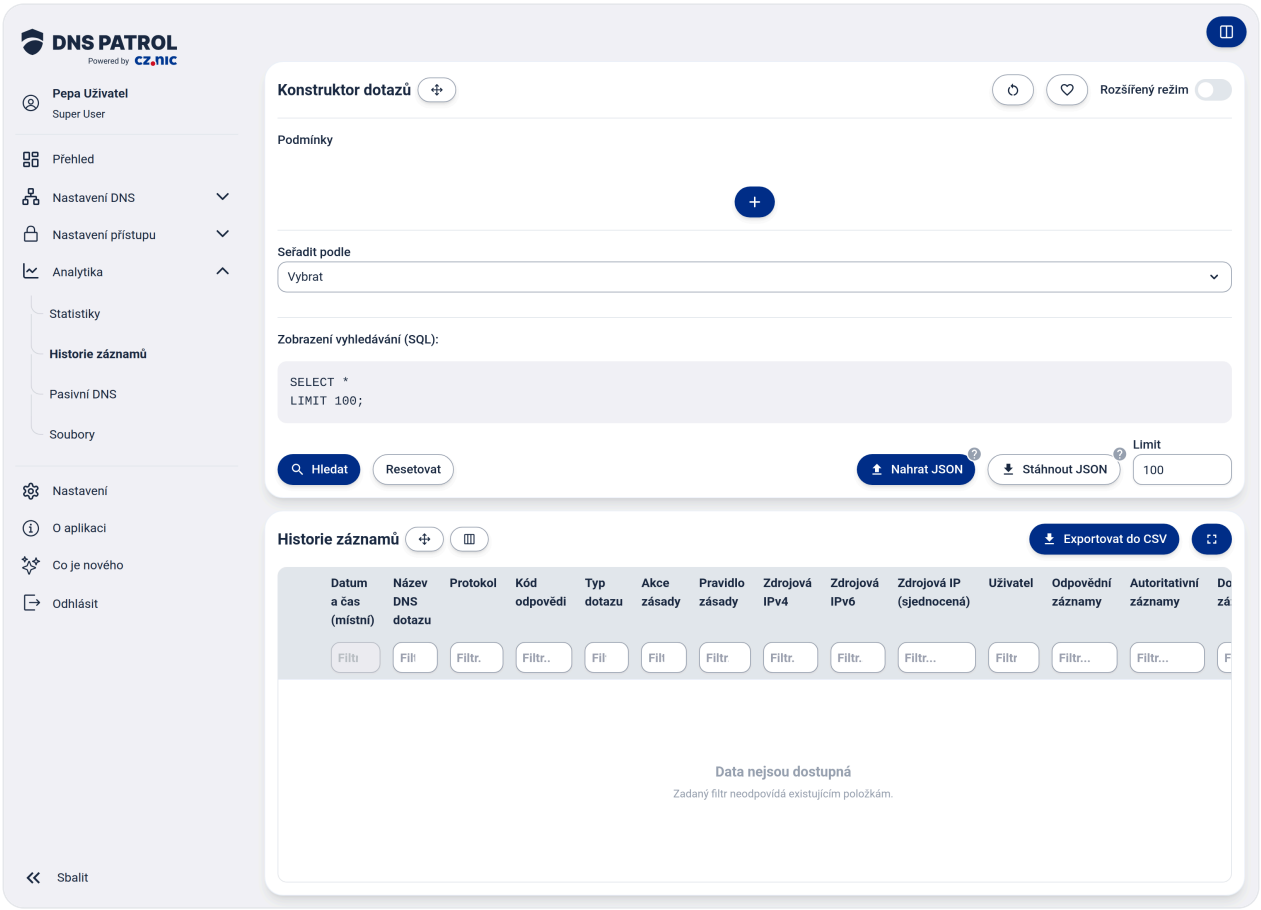


Obrázek 17 Stránka Statistiky s grafy za posledních 30 dní.

7.2 Historie záznamů

V této sekci lze pomocí filtrace získat archivní dotazy.

Vyhledávání funguje v režimu základním a rozšířeném. Základní režim umožňuje filtrování (s logickými spojkami) a řazení, rozšířený režim navíc podporuje agregace a filtrování v nich. V konstruktoru dotazů vytvoříte kýžený dotaz a nastavíte limit počtu výsledků, výsledky splňující podmínky jsou potom zobrazeny v tabulce níže. Rozšířený režim lze zapnout přepínačem v pravém horním rohu obrazovky.



Obrázek 18 Stránka Historie záznamů s konstruktorem dotazů.

Vyberte pole (rozšířený režim)

Určuje, jaké sloupce se zobrazí v tabulce. Ve výchozím režimu toto pole není vidět a zobrazí se všechny dostupné sloupce. V SQL odpovídá výrazu `SELECT [výběr]`.

Agregace (rozšířený režim)

Agregace vypočítávají jednu souhrnnou hodnotu z několika záznamů (často definovaných v **Seskupit podle**) a tuto hodnotu ukládají do nového pole. Agregaci lze definovat polem a funkcí, následně lze tomuto nově vytvořenému poli definovat alias.

Agregovat lze pouze podle vybraných polí (definovaných v **Vyberte pole**).

Agregace	Funkce
`COUNT`	Spočítá kolik je záznamů obsahujících nenulovou hodnotu pole (podporuje wildcard *)
`SUM`	Sečte numerické hodnoty v poli přes všechny záznamy (dostupné pouze pro numerické pole)
`AVG`	Vypočítá průměrnou hodnotu pole přes všechny záznamy (dostupné pouze pro numerické pole)
`MIN`	Najde nejmenší hodnotu v poli přes všechny záznamy (funguje pro čísla i řetězce)
`MAX`	Najde největší hodnotu v poli přes všechny záznamy (funguje pro čísla i řetězce)
`COUNT DISTINCT`	Spočítá kolik je **unikátních** nenulových záznamů pole
`MEDIAN`	Vypočítá medián (střední hodnotu) přes všechny záznamy (dostupné pouze pro numerické pole)
`STDDEV_POP`	Vypočítá populační směrodatnou odchylku - míra rozptylu numerických hodnot
`TO_START_OF_MINUTE`	Seskupí výsledky jiných definovaných agregací po minutách
`TO_START_OF_HOUR`	Seskupí výsledky jiných definovaných agregací po hodinách
`TO_START_OF_DAY`	Seskupí výsledky jiných definovaných agregací po dnech
`TO_START_OF_WEEK`	Seskupí výsledky jiných definovaných agregací po týdnech
`TO_START_OF_MONTH`	Seskupí výsledky jiných definovaných agregací po měsících
`TO_START_OF_QUARTER`	Seskupí výsledky jiných definovaných agregací po čtvrtletích
`TO_START_OF_YEAR`	Seskupí výsledky jiných definovaných agregací po rocích
`TO_START_OF_FIVE_MINUTES`	Seskupí výsledky jiných definovaných agregací po pěti minutách
`TO_START_OF_TEN_MINUTES`	Seskupí výsledky jiných definovaných agregací po deseti minutách
`TO_START_OF_FIFTEEN_MINUTES`	Seskupí výsledky jiných definovaných agregací po patnácti minutách

Ve výchozím režimu nejsou agregace dostupné.

Podmínky

Podmínky jsou aplikovány pro každý záznam ještě před agregací (pokud je aplikovaná). Podmínku lze aplikovat na libovolnou položku v záznamu. Při kliknutí na ikonku `plus -> přidat podmínku` vyberete pole, operátor a hodnotu. Výběr operátoru je určen typem daného pole, resp. pole typu číslo lze filtrovat matematickými operátory menší/větší než atp. a pole typu string lze filtrovat pomocí operátoru contains atp. Pole lze vždy filtrovat operátory `Rovná se`, `Nerovná se`, `Je prázdné (NULL)` a `Není prázdné`. V SQL odpovídá výrazu `WHERE`.

Jednotlivé podmínky lze seskupovat pomocí **skupin**. Skupinu lze vytvořit kliknutím na ikonku `plus -> přidat skupinu`. Skupina může obsahovat další vnořené skupiny, nebo podmínky. Podmínky/skupiny lze pak spojovat logickými spojkami AND/OR (a/nebo), které se objeví po přidání dvou či více podmínek/skupin. Logická spojka AND má přednost před OR.

Filtr	Funkce
Rovná se	Rovnost
Nerovná se	Nerovnost
Větší nebo rovno	Větší nebo rovno zadané hodnotě (pro číselné hodnoty)
Menší nebo rovno	Menší nebo rovno zadané hodnotě (pro číselné hodnoty)
Větší než	Větší než zadaná hodnota (pro číselné hodnoty)
Menší než	Menší než zadaná hodnota (pro číselné hodnoty)
Je v seznamu	Nachází se v seznamu hodnot
Není v seznamu	Nenachází se v seznamu hodnot
Obsahuje	Obsahuje zadaný podřetězec (pro textové hodnoty; u IP polí jde o porovnání podřetězce bez kontroly platnosti IP adresy)
Neobsahuje	Neobsahuje zadaný podřetězec (pro textové hodnoty; u IP polí jde o porovnání podřetězce bez kontroly platnosti IP adresy)
Začíná na	Začíná zadanou předponou (pro textové hodnoty)
Končí na	Končí zadanou příponou (pro textové hodnoty)
`Je prázdné (NULL)`	Je prázdná hodnota
Není prázdné	Není prázdná hodnota

Některá pole nabízejí jen část těchto operátorů. Pole Země přijímá pouze Rovná se, Nerovná se, `Je prázdné (NULL)` a Není prázdné. Pole se zdrojovou IP adresou (Zdrojová IPv4, Zdrojová IPv6) přijímají pouze operátory rovnosti, porovnání a seznamu. Pole Uživatel a Zařízení otevírají modální tabulku, ve které se jako hodnota podmínky vybere jedna či více entit; na jejich tlačítku je vidět, kolik položek je právě vybráno.

Podmínku s datem a časem lze zadat s přesností na sekundy.

Seskupit podle (rozšířený režim)

Seskupení kombinuje záznamy do skupin, kde má specifikované pole stejnou hodnotu. Lze vybrat pouze pole, která jsou vybraná (v Vyberte pole) nebo vytvořená v Agregace. Na tyto skupiny lze aplikovat další filtry v Having.

Having (rozšířený režim)

Having aplikují podmínky na seskupení vytvořené v Seskupit podle na rozdíl od podmínek, které se aplikují dříve a pro každý záznam.

Filtry se vytvářejí podobně jako v Podmínky, ovšem s tím rozdílem, že lze pouze vybrat pole definovaná v Agregace, nebo v Seskupit podle.

Seřadit podle

Určuje, podle jaké hodnoty výsledky řadit. Po vybrání daného pole lze kliknutím na tlačítko vedle názvu pole vybrat řazení sestupné/vzestupné.

Pokud uživatel aplikoval vybraná pole (`SELECT`) v rozšířeném režimu, lze filtrovat pouze podle těchto vybraných polí.

Zobrazení vyhledávání

Ukáže vytvořený dotaz ve formátu podobnému SQL. Slouží pouze k ilustrativním účelům, skutečně vypadá dotaz jinak (ve skutečnosti je spuštěný dotaz složitější, protože se k němu mimo jiné navíc aplikují přístupová práva dotazujícího se uživatele).

Limit, ukládání dotazů a vyhledávání

V pravém dolním rohu obrazovky lze aplikovat limit, tj. kolik výsledků bude z databáze získáno a zobrazeno. Tlačítkem ‘Stáhnout JSON’ lze jako soubor stáhnout aktuální dotaz. Ten lze později znovu použít jeho nahráním pomocí tlačítka ‘Nahrát JSON’

V levém dolním rohu lze nalézt tlačítka Hledat, které spustí vyhledávání a Resetovat, které smaže aktuální dotaz a vrátí vyhledávání do výchozího stavu.

Oblíbené dotazy

Dotaz, který používáte opakovaně, si lze uložit. Tlačítkem se srdcem v záhlaví konstruktoru dotazů se otevře okno s oblíbenými dotazy, kde se aktuální dotaz uloží pod zadaným názvem a volitelným popisem.

U každého uloženého dotazu jsou k dispozici tyto akce:

Akce	Popis
Použít	Načte uložený dotaz do konstruktoru
Aktualizovat aktuálním dotazem	Přepíše uložený dotaz tím, co je právě v konstruktoru
Sdílet	Otevře okno pro udělení oprávnění k dotazu dalším uživatelům
Smazat	Odstraní uložený dotaz

Název aktivního oblíbeného dotazu se zobrazuje přímo na tlačítku se srdcem, přejmenovat ho lze ikonou tužky vedle názvu. Pokud se dotaz v konstruktoru od uložené verze liší, je označen hvězdičkou jako neuložené změny; ty lze buď uložit, nebo zahodit a načíst uloženou verzi znovu.

Pokud uložený dotaz mezitím upraví jiný uživatel, portál na to upozorní a vypíše, které části se změnily. Vaše neuložené změny přitom zůstanou zachovány.

Vedle tlačítka s oblíbenými dotazy je tlačítko `Resetovat dotaz`, které vrátí konstruktor do výchozího stavu.

Sdílení odkazem

Adresa stránky vždy obsahuje aktuální dotaz i seznam zobrazených sloupců. Zkopírováním adresy z prohlížeče tak lze poslat kolegovi přesně to, co máte na obrazovce; po otevření odkazu se dotaz načte do konstruktoru. U velmi rozsáhlých dotazů může být odkaz příliš dlouhý, v takovém případě je vhodnější dotaz uložit jako oblíbený a nasdílet ho.

Tabulka historie záznamů

Po spuštění filtrace pomocí tlačítka Hledat se výsledky zobrazí v tabulce v spodní části stránky. Této tabulce lze přepínat stránky, pokud je výsledků více než v limitu. Výsledky lze také exportovat do souboru CSV

Nad tabulkou jsou tlačítka pro nastavení viditelnosti sloupců a pro přepnutí tabulky na celou obrazovku. Celou obrazovku lze ukončit stejným tlačítkem nebo klávesou Esc. Přidání sloupce si potřebná data načte samo, není nutné spouštět vyhledávání znovu.

Kontextové menu buňky

Kliknutím pravým tlačítkem na libovolnou buňku výsledků se otevře menu s těmito volbami:

Volba	Popis
Rovná se	Přidá do konstruktoru podmínku na hodnotu z buňky
Nerovná se	Přidá do konstruktoru podmínku vylučující hodnotu z buňky
Kopírovat hodnotu	Zkopíruje hodnotu buňky do schránky
Otevřít detail uživatele	Otevře stránku uživatele z daného řádku v nové záložce (jen u sloupce s uživatelem)
Přidat do sady pravidel	Zařadí doménu z daného řádku do vybrané sady pravidel (jen pokud je sloupec s doménou zobrazen)

Podmínka se do konstruktoru přidá s operátorem, který dané pole podporuje; u prázdné buňky se místo prvních dvou voleb nabídne `Je prázdné (NULL)`, resp. **Není prázdné**. Konstruktor se aktualizuje ihned, vyhledávání je pak nutné spustit tlačítkem Hledat.

Příklady kompletních dotazů

Tento dotaz zobrazí 500 (ne nutně posledních) záznamů s IP adresami dotazujícího v daném rozsahu.

```
SELECT *
WHERE Source IPv4 >= '192.168.0.0'
  AND Source IPv4 >= '220.0.0.0'
LIMIT 500;
```

Tento dotaz zobrazí poslední datum a čas, název DNS dotazu a počet unikátních klientů ze 100 záznamů takových, které splňují časovou nerovnost (v době psaní minulý týden) a které po seskupení mají alespoň 10 unikátních dotazujících. Tyto záznamy budou seřazeny sestupně podle počtu dotazů.

```
SELECT MAX(Datum a cas (místní)) AS last_seen,
       COUNTDISTINCT(Zdrojová IP (sjednocená)) AS unique_clients,
       Název DNS dotazu
WHERE Datum a cas (místní) >= 1762167600
GROUP BY Název DNS dotazu
HAVING unique_clients > 10
ORDER BY unique_clients DESC
LIMIT 100;
```

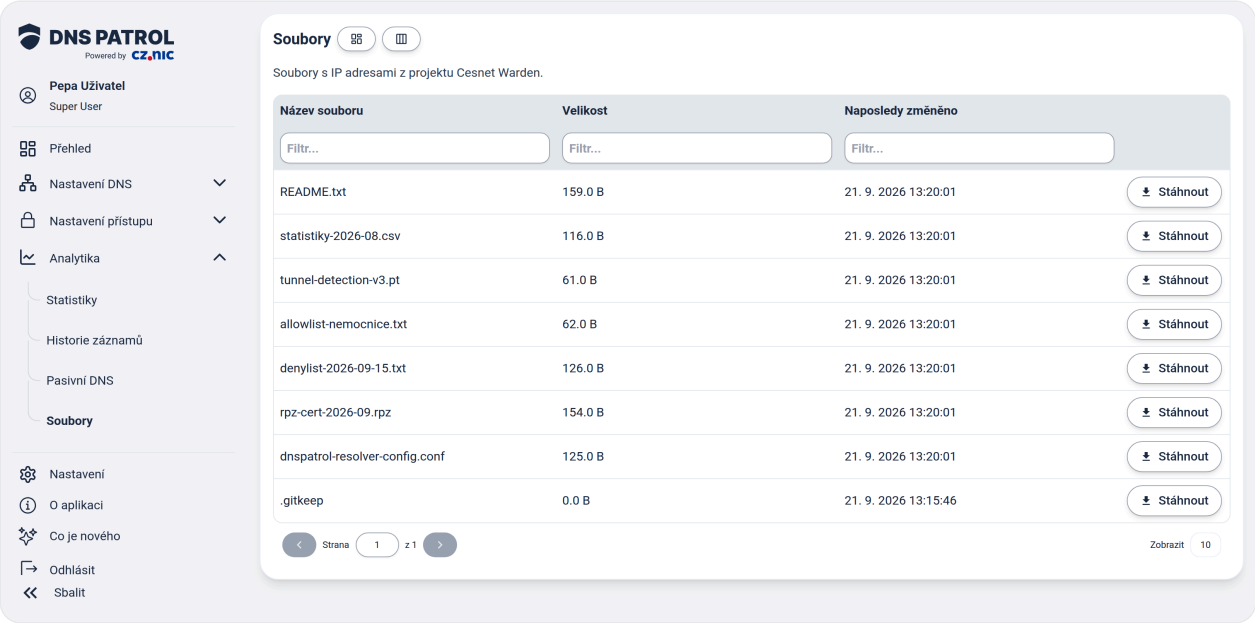
7.3 Pasivní DNS

Tato sekce slouží k sledování historie změn DNS záznamů. V pravém horním rohu lze zadat žádanou doménu spolu s typem záznamů. Odpovídající výsledky se zobrazí v tabulce:

Položka	Popis
Název záznamu	Vyhledaná doména
Typ záznamu	Typ DNS záznamu
Data odpovědi	Odpovídající data záznamu
Poprvé spatřen	Tento záznam byl poprvé spatřen v tento čas
Poslední výskyt	Tento záznam byl naposledy spatřen v tento čas
Počet	Udává, kolikrát resolver v daném časovém rozmezí zachytili v DNS odpovědích tento záznam

7.4 Soubory

V sekci soubory lze stáhnout seznamy podezřelých IP adres z projektu Cesnet Warden. Tyto seznamy pak lze použít například ve firewallu.



Obrázek 19 Tabulka souborů ke stažení.

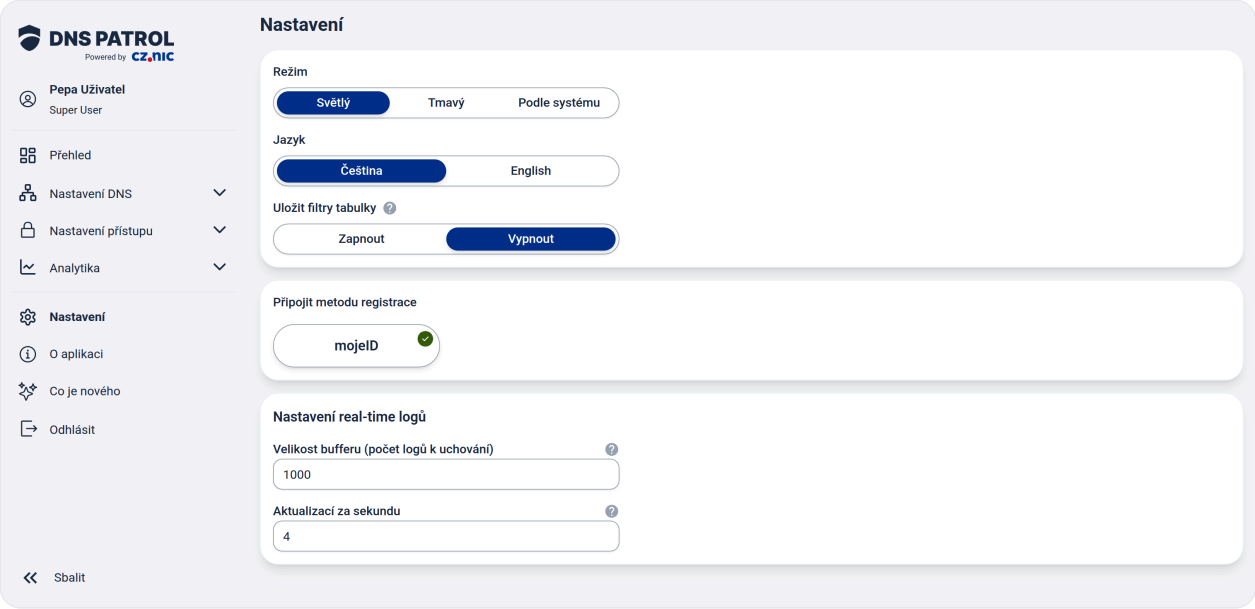
Položka	Popis
Název souboru	Název souboru
Velikost	Velikost souboru
Naposledy změněno	Čas poslední změny souboru
Akce	Tlačítko ke stažení daného souboru

Nastavení

V nastavení je možné zvolit jiný jazyk, barevný režim, nebo uživateli připojit jiný způsob přihlašování.

Volbou **Uložit filtry tabulky** se zapne automatické ukládání filtrů a řazení tabulek. Filtry a řazení se pak obnoví při návratu na stránku, ve výchozím stavu se po jejím opuštění zahodí.

Lze také nastavit velikost bufferů pro záznamy v reálném čase. Vyšší hodnoty zapříčiní ukládání více dat a častější obnovování výsledků na úkor většího vytížení paměti a procesoru.

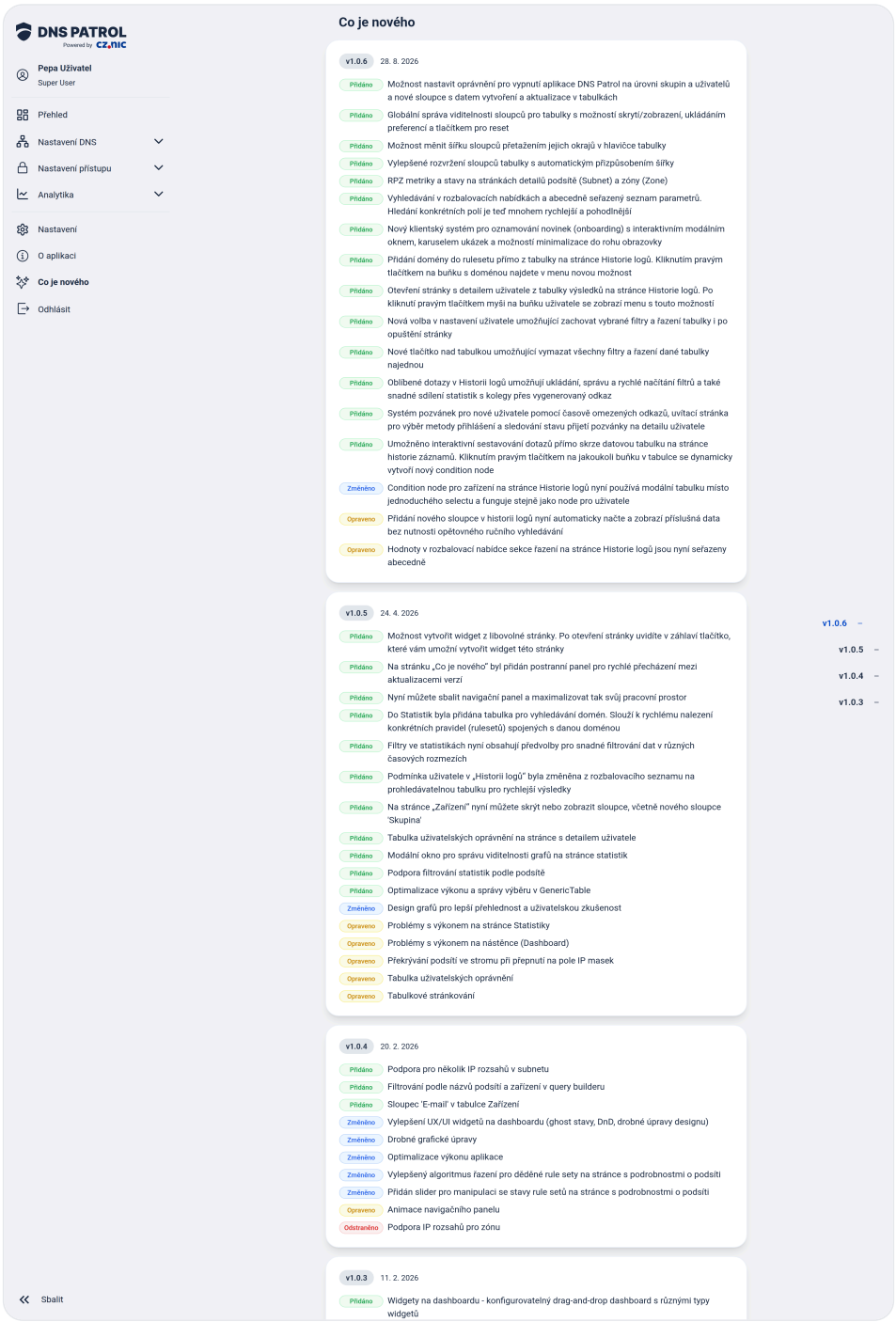


Obrázek 20 Stránka Nastavení.

Co je nového

Na této stránce je vidět přehled změn pro každou verzi aplikace.

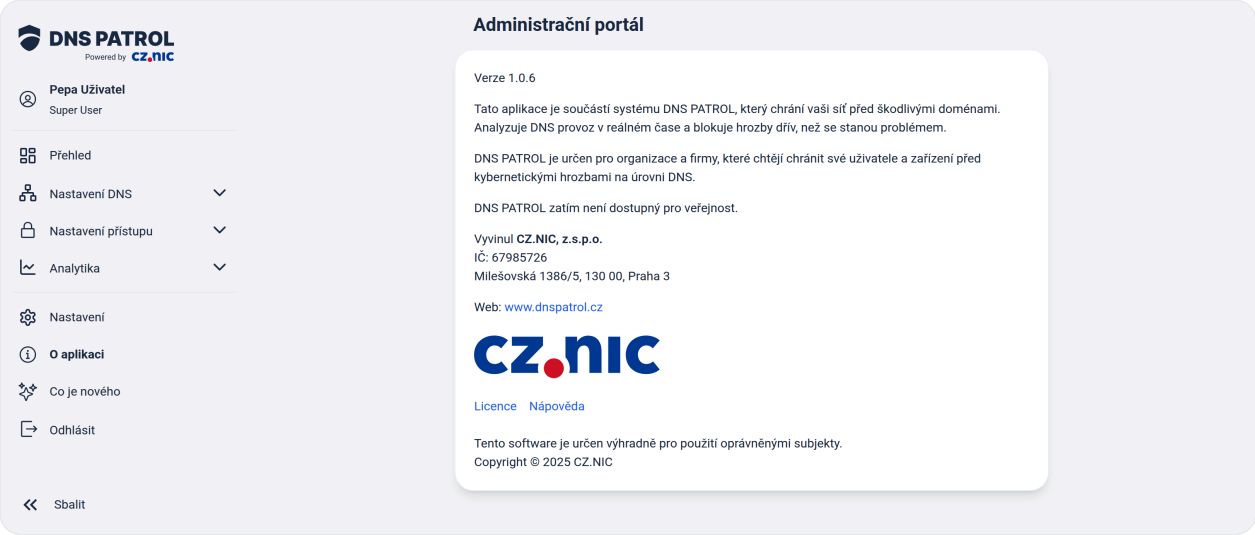
Stránka `Co je nového` obsahuje přehled změn v jednotlivých verzích administračního portálu - nové funkce, vylepšení, opravy chyb a odstraněné funkce. V pravé části stránky se nachází postranní panel se seznamem verzí, pomocí kterého lze rychle přeskočit na požadovanou verzi.



Obrázek 21 Stránka Co je nového s postranním panelem verzí.

O aplikaci

Obsahuje informace o aplikaci, jako aktuální verzi, odkazy na dokumentaci, atp.



Obrázek 22 Stránka O aplikaci.

Klientské aplikace

Klientská aplikace slouží koncovým zařízením, která se pohybují mimo síť organizace. Po registraci směruje veškerý DNS provoz zařízení na unikátní DoH URL externí zóny, takže se na dotazy uplatní stejné sady pravidel jako uvnitř sítě.

Zařízení se registruje jednorázovým registračním kódem, který uživateli vystaví administrátor v portálu. Kód je osmimístný a skládá se z velkých písmen a číslic. Po jeho ověření se zařízení objeví v portálu v sekci **Nastavení přístupu** > **Zařízení**.

Aplikace nemá žádné další nastavení. Nastavení zařízení určuje výhradně konfigurace v administračním portálu.

11.1 Obsah

iOS – Aplikace pro iPhone a iPad Android – Aplikace pro telefony a tablety s Androidem Windows – Aplikace pro počítače s Windows

iOS

Aplikace pro iPhone a iPad se instaluje z App Store. Na iOS se DNS provoz nesměruje přes VPN, ale přes systémové rozhraní pro DNS proxy, které je nutné po instalaci ručně aktivovat.

Obrázek 23 DNS PATROL v App Store.

12.1 První spuštění

Po prvním spuštění aplikace vyžaduje registrační kód, který vydává administrátor z administračního portálu. Kód je osmimístný, skládá se z velkých písmen a číslic a vkládá se po znacích do políček pod nadpisem **Zadejte registrační kód**. Tlačítkem **Odeslat** se kód ověří a aplikace přejde na hlavní stránku.

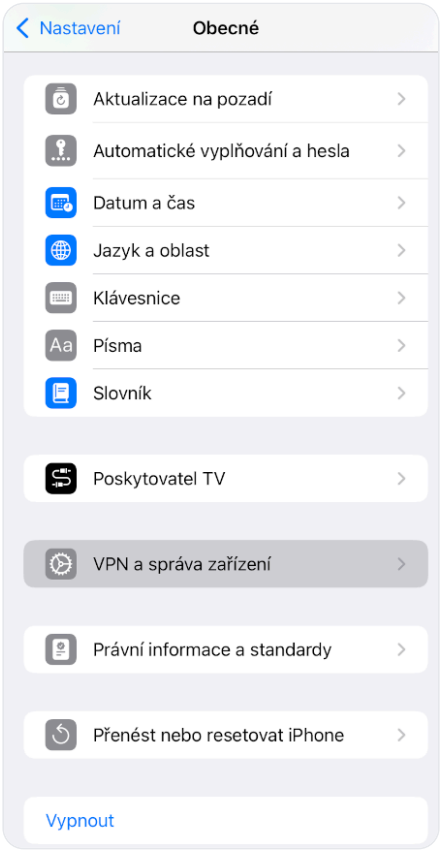
Obrázek 24 Zadání registračního kódu po prvním spuštění.

12.2 Aktivace nastavení DNS

Samotná registrace provoz zařízení ještě nepřesměruje. DNS PATROL je nutné vybrat jako DNS v systémovém nastavení. Zkrácený postup je dostupný i v aplikaci pod odkazem **Jak aktivovat**.

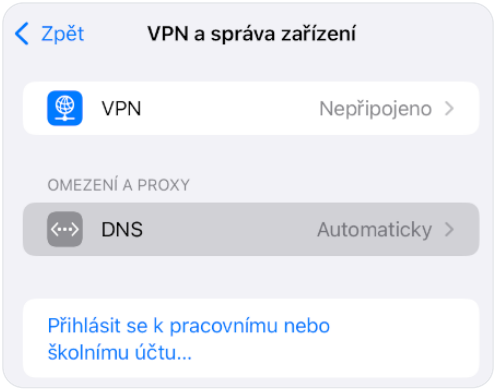
Obrázek 25 Nápověda `Jak aktivovat` v aplikaci.

V aplikaci `Nastavení` otevřete sekci `Obecné` a zvolte `VPN a správa zařízení`.



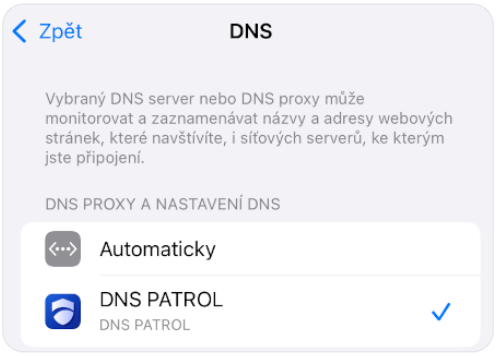
Obrázek 26 Nastavení > Obecné > VPN a správa zařízení.

V sekci `OMEZENÍ A PROXY` rozklikněte `DNS`.



Obrázek 27 Položka DNS je ve výchozím stavu nastavená na Automaticky.

V sekci **DNS PROXY A NASTAVENÍ DNS** vyberte **DNS PATROL**.



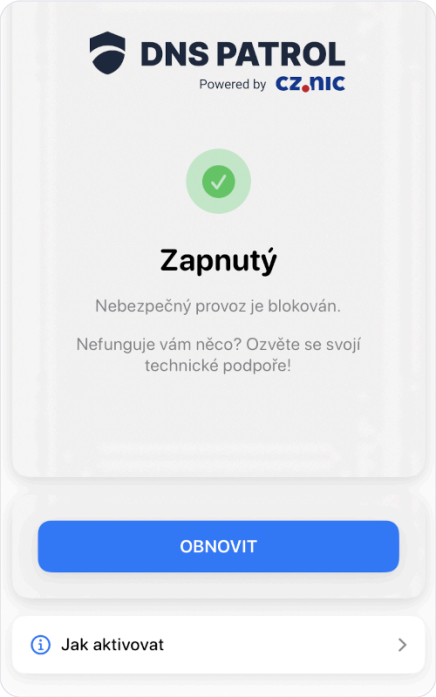
Obrázek 28 Výběr DNS PATROL místo automatického nastavení.

Tím je DNS PATROL na zařízení aktivní. Nastavení lze ověřit návratem do aplikace, kde se stav změní na **Zapnutý**.

12.3 Hlavní stránka

Hlavní stránka ukazuje aktuální stav služby:

Stav	Popis
Zapnutý	DNS PATROL je vybraný jako DNS zařízení a nebezpečný provoz je blokován
Vypnutý	DNS PATROL není aktivní, dotazy zpracovává výchozí DNS zařízení



Obrázek 29 Stav Zapnutý.

Obrázek 30 Stav Vypnutý.

Tlačítko **Obnovit** znovu načte stav služby, například po změně v systémovém nastavení. Odkaz **Jak aktivovat** rozbalí postup pro aktivaci nastavení DNS.

12.4 Smazání dat aplikace

Aplikace na iOS neumožňuje data vymazat zevnitř. Pokud je potřeba zařízení zaregistrovat znovu, tedy zadat jiný registrační kód, je nutné aplikaci odinstalovat a nainstalovat z App Store znovu.

Původní záznam o zařízení zůstává v portálu v sekci **Nastavení přístupu** > **Zařízení**, odkud ho lze smazat.

12.5 Hlášení potíží

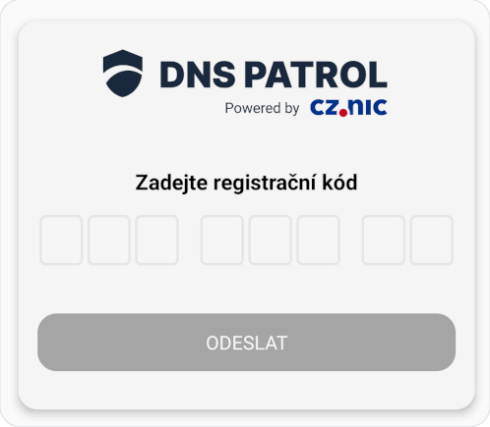
Problémy s aplikací nebo s nedostupností webových stránek a aplikací řeší IT podpora organizace.

Android

Aplikace pro telefony a tablety s Androidem se instaluje z obchodu Google Play. DNS provoz zařízení směruje přes lokální VPN, kterou aplikace vytváří na zařízení. Provoz tedy neopouští zařízení přes VPN server, rozhraní slouží pouze k zachycení DNS dotazů.

13.1 První spuštění

Po prvním spuštění aplikace vyžaduje registrační kód, který vydává administrátor z administračního portálu. Kód je osmimístný, skládá se z velkých písmen a číslic a vkládá se po znacích do políček pod nadpisem **Zadejte registrační kód**. Tlačítkem **Odeslat** se kód ověří a aplikace přejde na hlavní stránku.

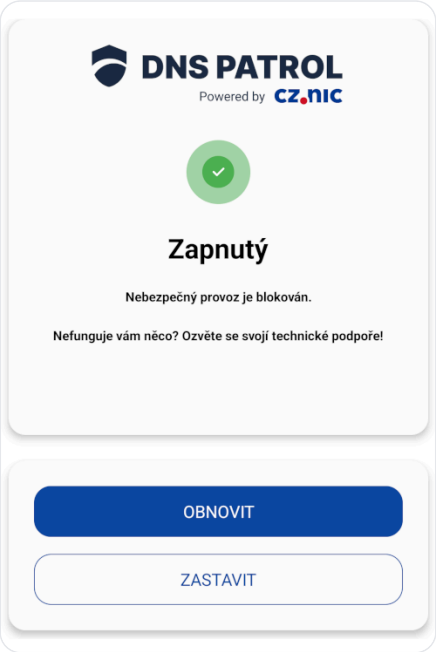


Obrázek 31 Zadání registračního kódu po prvním spuštění.

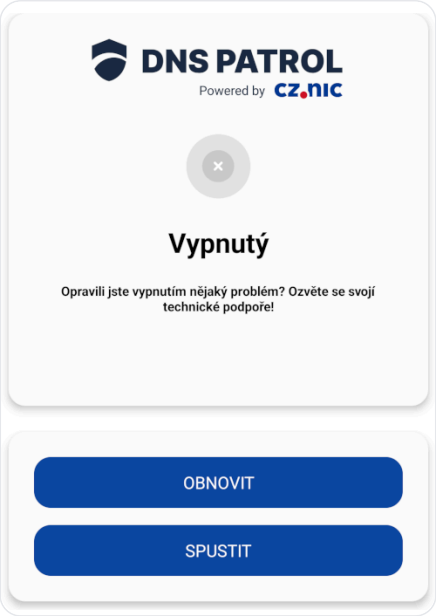
13.2 Hlavní stránka

Hlavní stránka ukazuje aktuální stav služby:

Stav	Popis
Zapnutý	DNS PATROL běží a nebezpečný provoz je blokován, na oznamovací liště je vidět ikona klíče
Vypnutý	DNS PATROL neběží, dotazy zpracovává výchozí DNS zařízení



Obrázek 32 Stav Zapnutý.



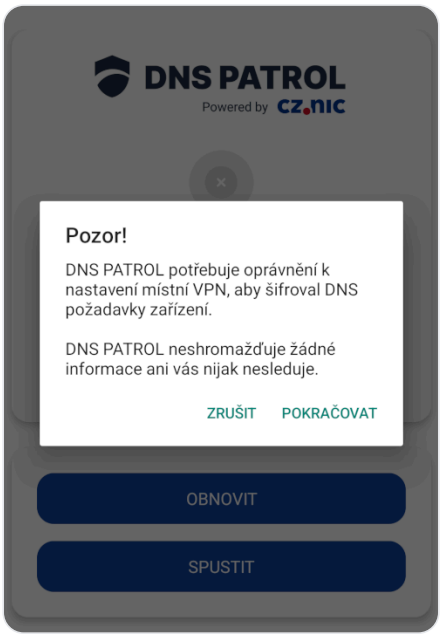
Obrázek 33 Stav Vypnutý.

Podle stavu jsou dostupná tlačítka:

Tlačítko	Funkce
Obnovit	Znovu načte stav služby
Zastavit	Zastaví běžící DNS PATROL (stav `Zapnutý`)
Spustit	Spustí DNS PATROL (stav `Vypnutý`)

13.3 Spuštění a oprávnění

Při prvním kliknutí na `Spustit` aplikace upozorní, že potřebuje oprávnění k nastavení lokální VPN pro šifrování DNS dotazů zařízení. Spuštění pokračuje tlačítkem `Pokračovat`.

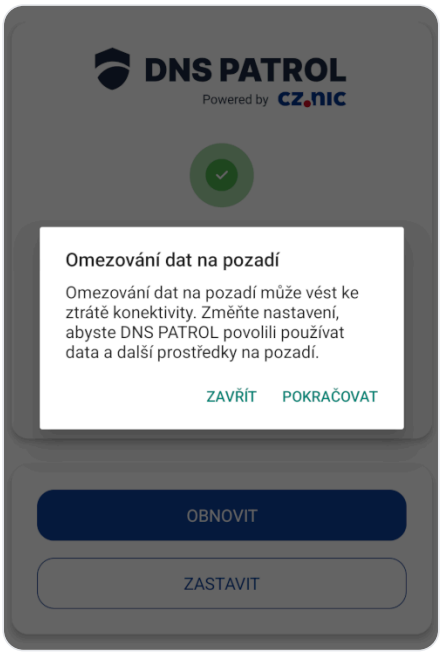


Obrázek 34 Upozornění na oprávnění k nastavení VPN.

Následuje systémový dialog **Žádost o připojení**, kterým Android žádá o povolení VPN. Potvrzuje se tlačítkem `OK`.

Obrázek 35 Systémová žádost o povolení VPN připojení.

Pokud aplikace nemá povolená data na pozadí, upozorní na to další dialog. Omezení dat na pozadí může vést ke ztrátě konektivity, protože aplikace nemůže DNS provoz obsluhovat, když neběží v popředí. Tlačítko **Pokračovat** otevře systémové nastavení **Využití baterie aplikací**, kde se přepínačem **Povolit používání aplikace na pozadí** omezení zruší.



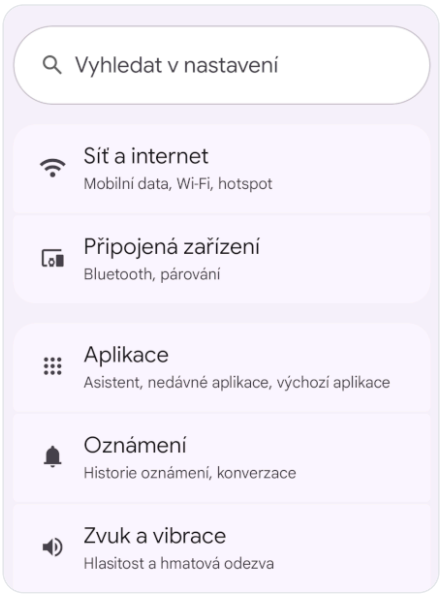
Obrázek 36 Upozornění na omezování dat na pozadí.

Obrázek 37 Povolení běhu aplikace na pozadí v nastavení zařízení.

13.4 Smazání dat aplikace

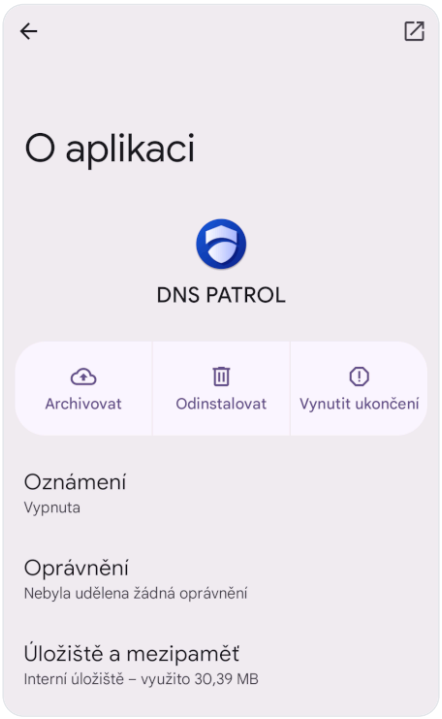
Pokud je potřeba zařízení zaregistrovat znovu, tedy zadat jiný registrační kód, lze buď aplikaci odinstalovat a nainstalovat z Google Play znovu, nebo rychleji vymazat její úložiště.

V nastavení zařízení zvolte `Aplikace`.



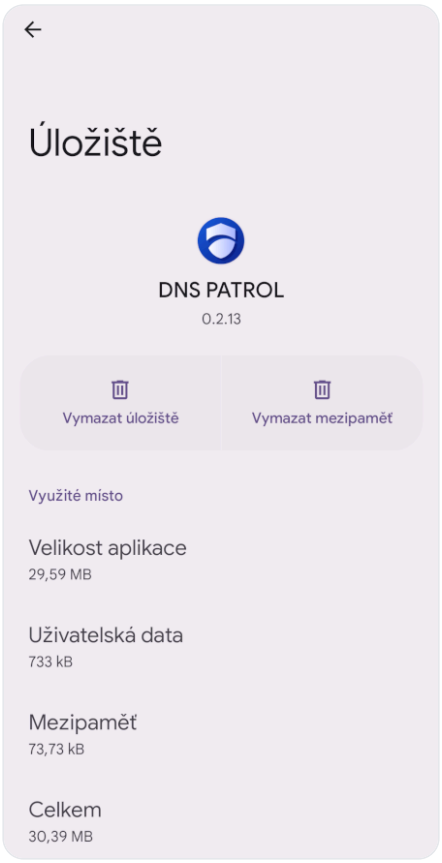
Obrázek 38 Nastavení zařízení.

Ze seznamu vyberte aplikaci DNS PATROL. Odtud ji lze tlačítkem **Odinstalovat** odebrat ze zařízení. Pro vymazání dat pokračujte na **Úložiště a mezipaměť**.



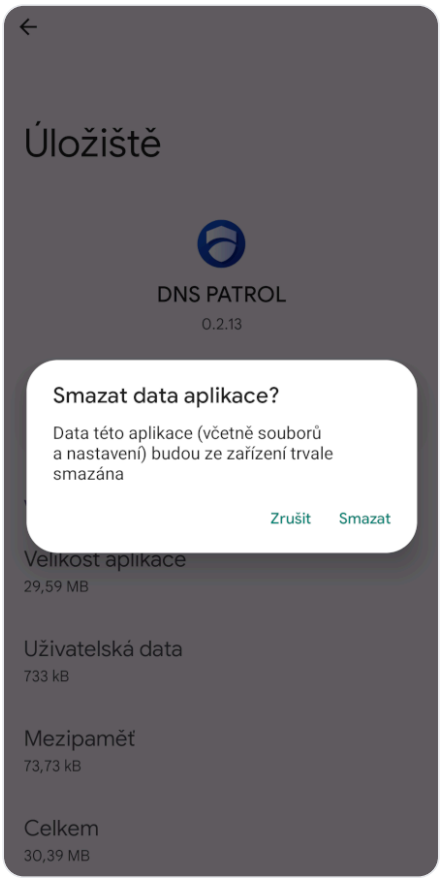
Obrázek 39 Informace o aplikaci DNS PATROL.

Zvolte **Vymazat úložiště**.



Obrázek 40 Úložiště aplikace.

Zobrazený dialog potvrďte tlačítkem **Smazat**. Při dalším spuštění bude aplikace znovu vyžadovat registrační kód.



Obrázek 41 Potvrzení smazání dat aplikace.

Původní záznam o zařízení zůstává v portálu v sekci **Nastavení přístupu** > **Zařízení**, odkud ho lze smazat.

13.5 Hlášení potíží

Problémy s aplikací nebo s nedostupností webových stránek a aplikací řeší IT podpora organizace.

Windows

Aplikace pro Windows se skládá z okna pro obsluhu a ze systémové služby `DnsPatrolAgent`, která běží na pozadí. Služba provozuje lokální DNS proxy na adrese `127.0.0.1` a přeposílá dotazy na DoH URL přidělenou zařízení. Po zapnutí ochrany se síťovým rozhraním staticky nastaví `127.0.0.1` jako DNS server, po vypnutí se rozhraní vrátí zpět na DNS z DHCP.

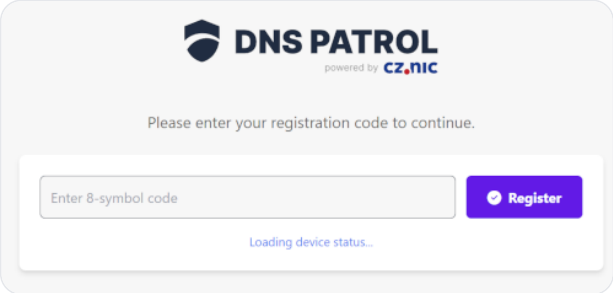
Rozhraní aplikace je pouze v angličtině.

14.1 Instalace

Instalace se spouští instalátorem, který vyžaduje potvrzení dialogu o povolení změn v počítači. Po dokončení instalace doporučujeme počítač restartovat.

14.2 První spuštění

Po prvním spuštění aplikace vyžaduje registrační kód, který vydává administrátor z administračního portálu. Kód je osmimístný, skládá se z velkých písmen a číslic a vkládá se do pole pod textem `Please enter your registration code to continue`. Tlačítkem `Register` se kód ověří a aplikace přejde na hlavní stránku.

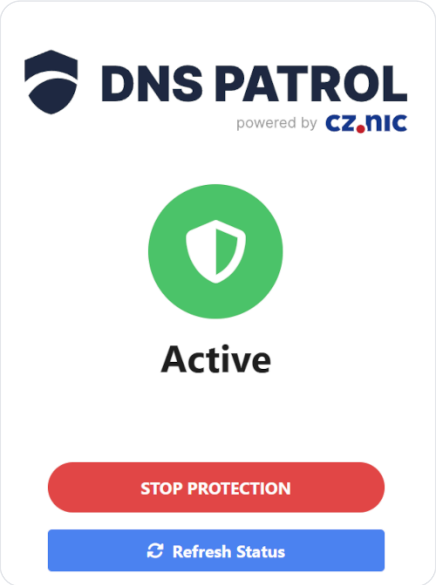


Obrázek 42 Zadání registračního kódu po prvním spuštění.

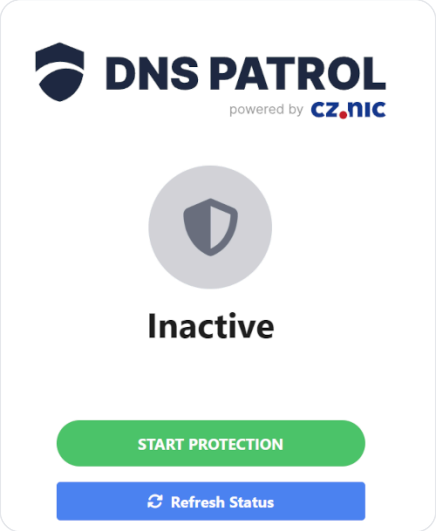
14.3 Hlavní stránka

Hlavní stránka ukazuje aktuální stav ochrany:

Stav	Popis
Active	DNS PATROL běží a nebezpečný provoz je blokován
Inactive	DNS PATROL neběží, dotazy zpracovává DNS server z DHCP



Obrázek 43 Stav Active.



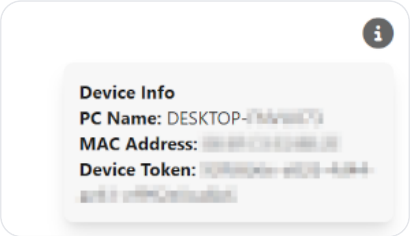
Obrázek 44 Stav Inactive.

Podle stavu jsou dostupná tlačítka:

Tlačítko	Funkce
Stop protection	Vypne ochranu a vrátí nastavení DNS na DHCP (stav `Active`)
Start protection	Zapne ochranu (stav `Inactive`)
Refresh Status	Znovu načte stav služby

14.4 Informace o zařízení

Informační ikona v pravém horním rohu zobrazí po najetí kurzorem údaje, pod kterými je zařízení vedené v portálu – jméno počítače, MAC adresu a token zařízení. Stejné zařízení lze v portálu dohledat v sekci `Nastavení přístupu` > `Zařízení`.



Obrázek 45 Informace o zařízení.

14.5 Odinstalace

Aplikaci odinstalujte až ve stavu `Inactive`. Odinstalátor zastaví a odebere službu `DnsPatrolAgent`, ale nastavení DNS na síťových rozhraních už nevrací zpět. Při odinstalaci ve stavu `Active` proto rozhraním zůstane staticky nastavená adresa `127.0.0.1`, na které po odebrání služby nic neposlouchá, a překlad jmen na počítači přestane fungovat.

14.6 Hlášení potíží

Problémy s aplikací nebo s nedostupností webových stránek a aplikací řeší IT podpora organizace. Pokud aplikace nefunguje hned po instalaci, zkuste nejprve počítač restartovat.