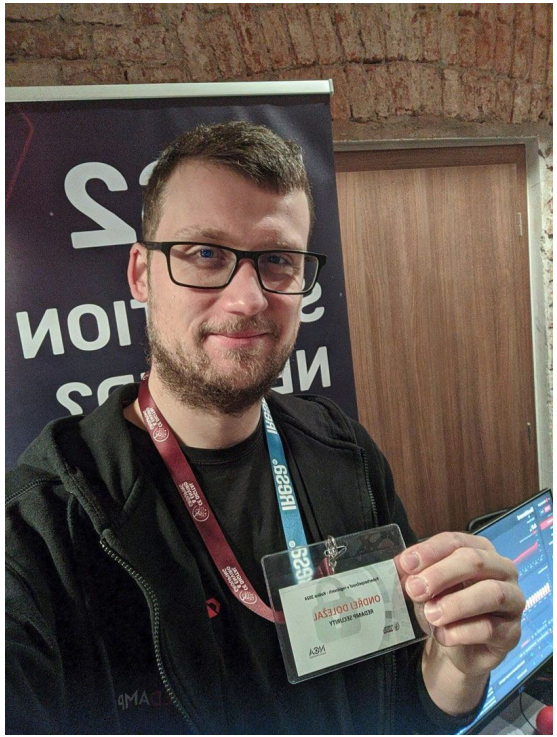
Bezpečné DNS doma i na cestách

Ondřej Doležal

OpenAlt
3.11.2024
FIT VUT v Brně

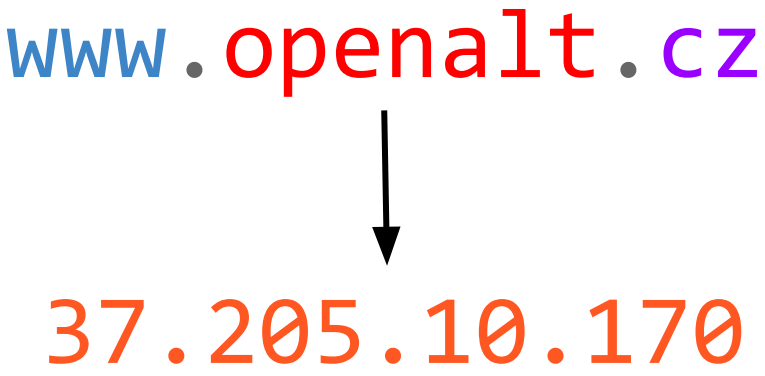
Kdo jsem

- profesně:
  - systémový administrátor v Redamp.io
- osobně:
  - kyberbezpečnost
  - počítačové sítě
  - IoT
  - soukromí na internetu.
- kontakty: https://www.odolezal.cz



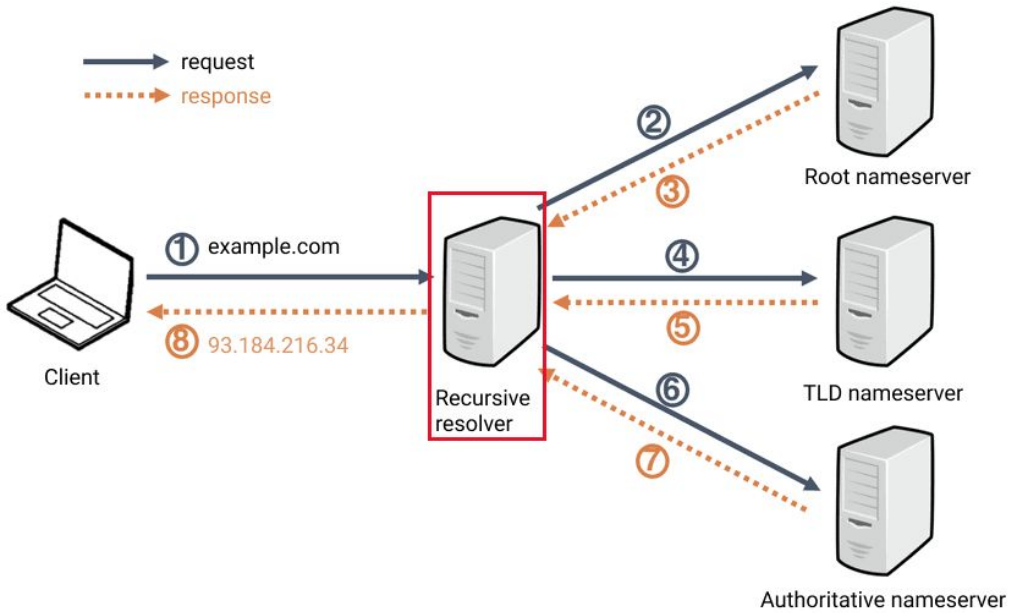
Co je DNS

- **D**omain **N**ame **S**ystem
- decentralizovaný systém doménových jmen
- jeden z pilířů internetu
- potřeba překladu **doménového jména** na IP adresu
- několik úrovní
- různé koncovky (tzv. TLD)



Jak funguje vyhledávání

- získání IP adresy pro “example.com” tzv. **rekurzivním vyhledáváním**
- rekurzivní resolver je většinou i **cachující**
- DNS forwarder
  - neprovádí vyhledávání
  - dotaz přepošle tzv. **upstream** serveru
  - většinou obsahuje i cache
  - součást LAN



Zdroj: https://blog.raidboxes.io/en/webdesign-development/domain-name-system-dns/

Bezpečné DNS

filtrované

- ochrana proti **škodlivým doménám**

šifrované

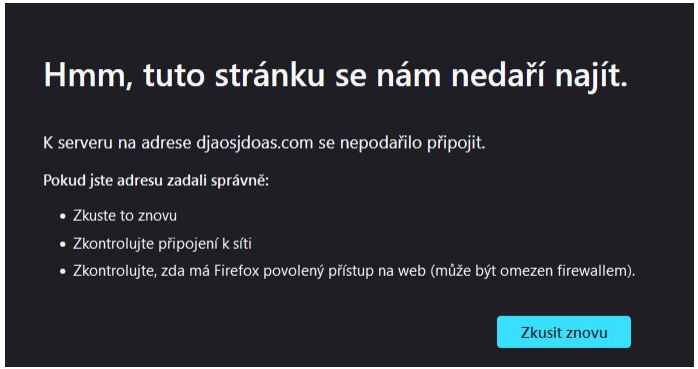
- ochrana proti **odposlechnutí komunikace**

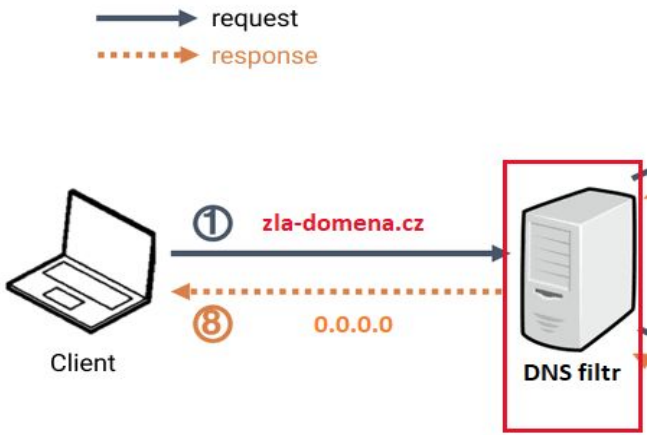
Jak to vypadá v praxi

- většina DNS provozu je:
  - **bez filtrování**
    - kromě legislativních požadavků (např.: “Seznamu nepovolených internetových her”)
  - **bez šifrování**
    - odposlech po cestě
    - statistika pro Cloudflare resolver: v ČR je **jen 17,5%** požadavků šifrovaných
- DNS servery vám automaticky nastavuje váš provider
  - IP adresy DNS serverů v rámci automatické konfigurace
- oblíbené Google DNS 8.8.8.8 domény nefiltruje

Podstata blokování

1. klient požádá o překlad “zla-domena.cz”
2. DNS filtr odpoví **blokovací odpovědí** na místo validní IP adresy
   a. blokovací odpověď je IP adresa “0.0.0.0” nebo speciálním typem DNS odpovědi
3. klient dostane **nesprávnou IP adresu**
4. výsledkem je **nezobrazená** stránka





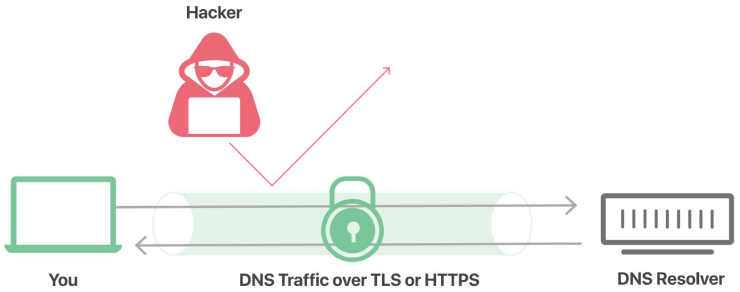
Proč to chtít?

- blokování **phishingu**
  - obecné doporučení je “neklikat na odkaz”
  - blokování domén jako sekundární obrana
- blokování **malware**
  - infrastruktura závislá na doménách
  - zablokování domény může zastavit napadení systému
    - Případ WannaCry (2017): doména jako “killswitch”
- ochrana **soukromí**
  - reklamy, tracking uživatele
  - uživatelská telemetrika (OS, Smart TV,...)
- blokování **nevhodného obsahu**
  - 18+ obsah na internetu
  - sociální sítě

Zdroj: https://bezpecnejsi.ostrava.cz/situace/internet/phishing-utoky-pres-zpravy/

Šifrované DNS

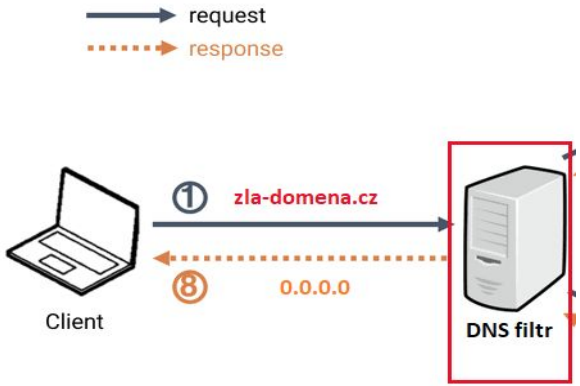
- **chrání soukromí** při odposlechu “po cestě”
- vytváří **šifrované spojení** z koncového zařízení k resolveru
- DNS over TLS (DoT)
  - klasická struktura DNS, které se pošle přes zabezpečené TLS spojení
  - TCP port 853 (lze snadno zablokovat na firewallu)
  - ověření serveru certifikátem
  - nativní podpora v Android telefonech, moderní routery, resolvery,...
- DNS over HTTPS (DoH)
  - binární forma i moderní JSON poslány přes HTTP/2
  - TCP port 443 (hůř se blokuje)
  - ověření serveru certifikátem
  - uživatelsky zajímavější (propagují hlavně prohlížeče)



Veřejné resolvery

Veřejné resolvery

- blokující veřejný resolver = **resolver** + **DNS filtr**
- vhodné pro “netechnické” uživatele
- nevyžadují žádnou registraci
- zamýšlený princip: “nastav a využívej”
- zdarma



Cloudflare

- renomovaný poskytovatel internetových služeb: cloud, proxy, ...
- robustní infrastruktura po celém světě
  - dlouhodobě jeden z **nejrychlejších** resolverů na světě
- vlastní aplikace 1.1.1.1 WARP
  - **automaticky** implementuje bezpečné DNS na vašem zařízení
- resolver na IP adrese 1.1.1.1 **neposkytuje** filtrování!
- **1.1.1.1 for Families**
  - 1.1.1.2 - malware filtr
  - 1.1.1.3 - malware + “adult” filtr
- podpora DoT, DoH (+HTTP/3), IPv6, DNSSEC
- logovací politika: anonymizováno (neuchovává osobní data)
- právní rámec: USA

1.1.1.1
FOR FAMILIES

Quad9

- neziskový projekt Quad9 Foundation (komerční i nekomerční subjekty)
- resolver se zaměřením na **soukromí** a ochranu před malwarem phishingem
- v provozu od 2016
  - dlouhodobě stabilní výsledky (viz srovnání dále)
- celosvětová infrastruktura
- vlastní aplikace “Quad9 Connect” (aktuálně není v app storech)
- podpora DoT, DoH, DoQ, DNSCrypt, IPv6, DNSSEC
- chybí “adult” filtr
- logovací politika: anonymizováno, meta data k výzkumu
- právní rámec: Švýcarsko

dns0.eu

- neziskový projekt od autorů NextDNS (založeno 2022 ve Francii)
- **protiváha** k USA resolverům Google a Cloudflare
- snaha nabídnout službu 100% kompatibilní s EU legislativou
  - infrastruktura čistě v EU (server v každé členské zemi)
- velký počet zdrojů škodlivých domén, spolupráce napříč komunitou
- nemá vlastní aplikaci pro mobilní telefony
- varianta “**Zero**” pro “vysoce citlivé prostředí”, aka. “hard core” blokování
- varianta “**Kids**” pro blokování “adult” obsahu
  - 18+ stránky, explicitní výsledky, dospělý obsah na YouTube, seznamky, smíšený obsah, warez
- podpora DoT, DoH (+HTTP/3), DoQ, IPv6, DNSSEC
- logování: anonymizováno, meta data k výzkumu
- právní rámec: EU

Srovnání veřejných resolverů

Měření *Nexxwave.eu*: Vzorek **233 539 škodlivých domén** z CERT.pl a URLhaus

Resolver	Zablokováno domén
dns0.eu Zero	99,14 %
dns0.eu	99,12 %
Quad9	98,08 %
Cloudflare for Families	3,93 %
Google Public DNS	0,22 %

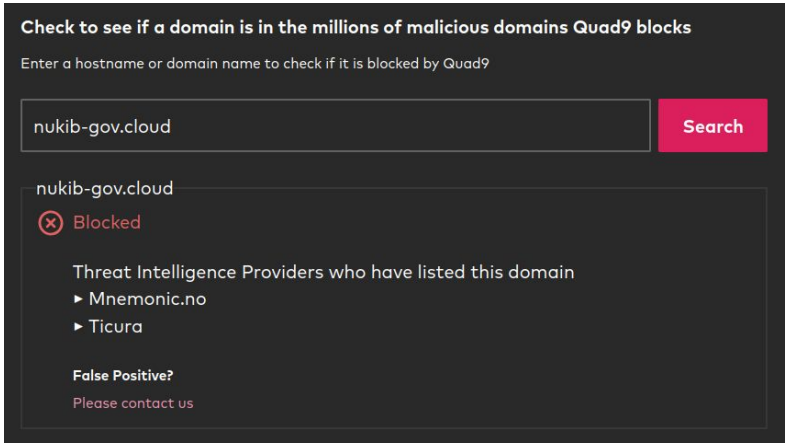
Zdroj dat, včetně metodiky měření: https://techblog.nexxwave.eu/public-dns-malware-filters-tested-in-september-2024/

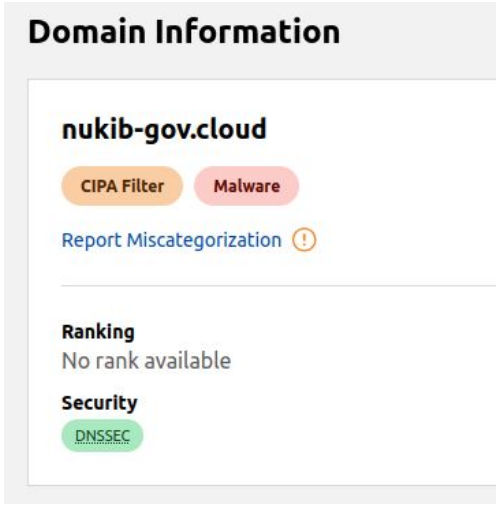
Nová doména

NÚKIB › Infoservis › Hrozby › Upozorňujeme na zneužívání identit Amazon, Microsoft a českých institucí

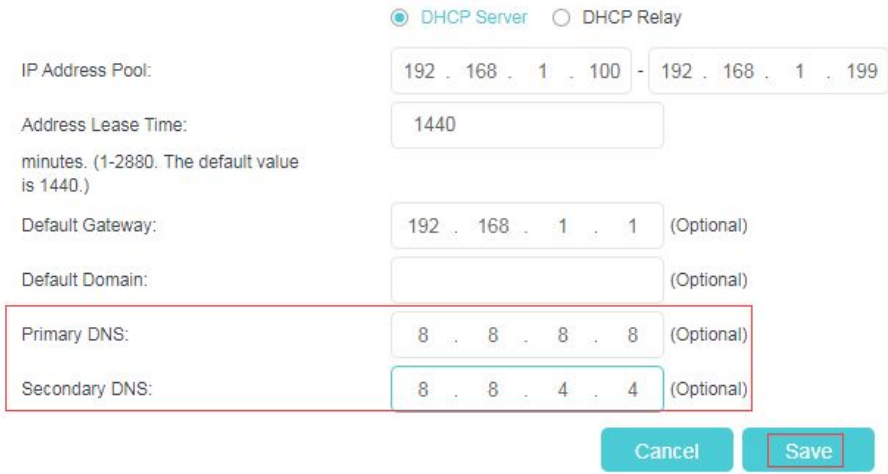
Upozorňujeme na zneužívání identit Amazon, Microsoft a českých institucí

24. říjen 2024





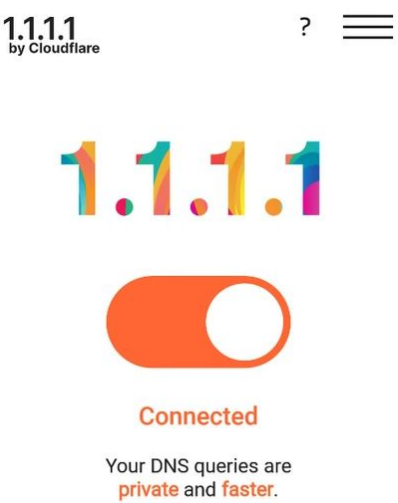
Nastavení na routeru

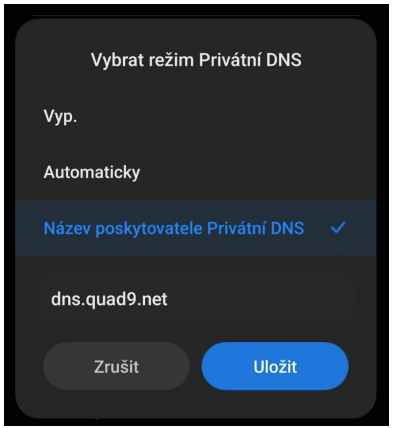


- výhoda: jednoduché, pro celou LAN
  - Řeší “hloupá” zařízení (IoT, Smart TV)
- nevýhoda:
  - bez šifrování

Nastavení na mobilu

- Android
  - aplikace (Cloudflare, Quad9,...) na Google Play
    - velmi jednoduché nastavení typu “klikni a funguj”
  - funkce **Privátní DNS**
    - defakto DoT
    - nutné manuálně nakonfigurovat
- iOS
  - aplikace (Cloudflare, Quad9,...) na App Store
    - velmi jednoduché nastavení typu “klikni a funguj”
  - DNS Profile
    - nutné vytvořit .mobileconfig konfigurační soubor
    - dostupné online
    - velké resolvery mají svoje konfigurace podepsané





Nastavení na počítači

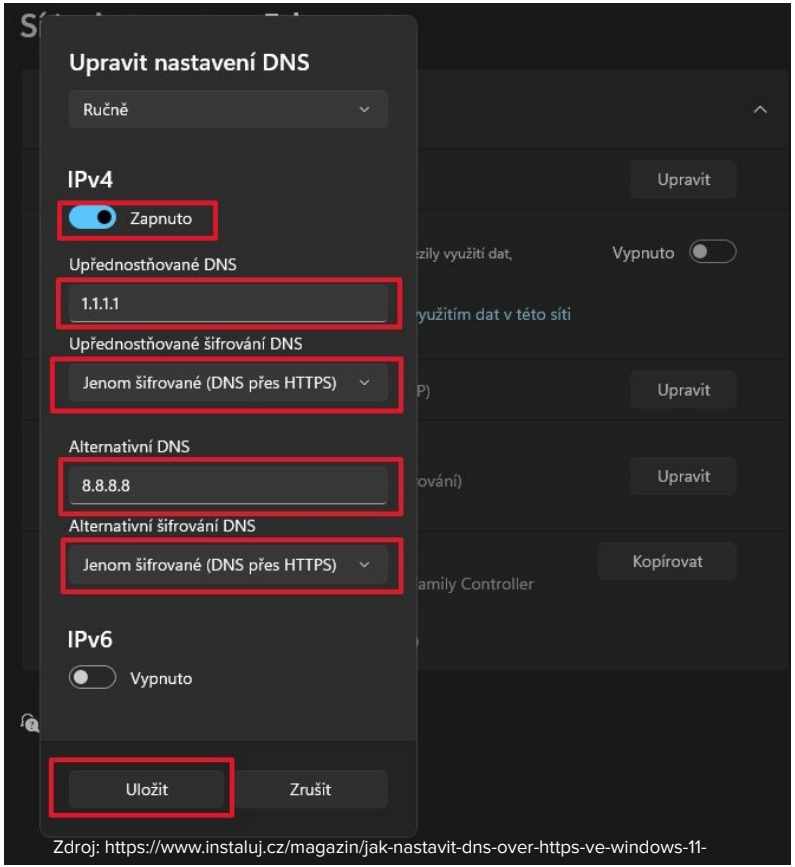
- aplikace nejsou příliš rozšířené
- šifrované spojení ze zařízení k resolveru
- podpora ve **Windows 11**
- **Linux**: systemd-resolved podporuje DoT

1. Enable the systemd-resolved service.

2. In /etc/systemd/resolved.conf, add the following:

```
[Resolve]
DNS=193.110.81.0#dns0.eu
DNS=2a0f:fc80::#dns0.eu
DNS=185.253.5.0#dns0.eu
DNS=2a0f:fc81::#dns0.eu
DNSOverTLS=yes
```

3. Restart the systemd-resolved service.



Zdroj: https://www.instaluj.cz/magazin/jak-nastavit-dns-over-https-ve-windows-11-

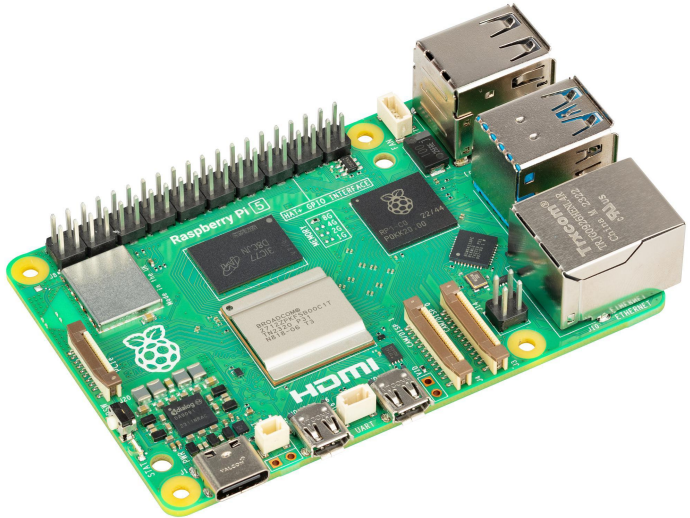
Výhody X Nevýhody

- Výhody
  - šifrované spojení ze zařízení k resolveru
  - podpora moderních protokolů
  - funguje kdekoliv
- Nevýhody
  - potenciálně problém s lokální politikou sítě
    - překlad interních domén nebude fungovat (hlavně firemní sítě)
    - “captive” portály můžou mít problém

Vlastní řešení

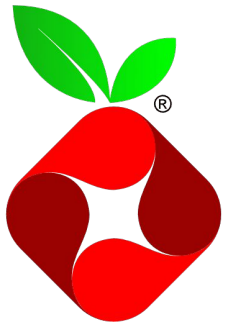
Vlastní řešení

- pokud si rádi hrajete, DIY
- náročnější na provoz (vlastní HW), údržba
- časová investice
- plná kontrola nad filtrováním, logování dotazů, doplňkové funkce



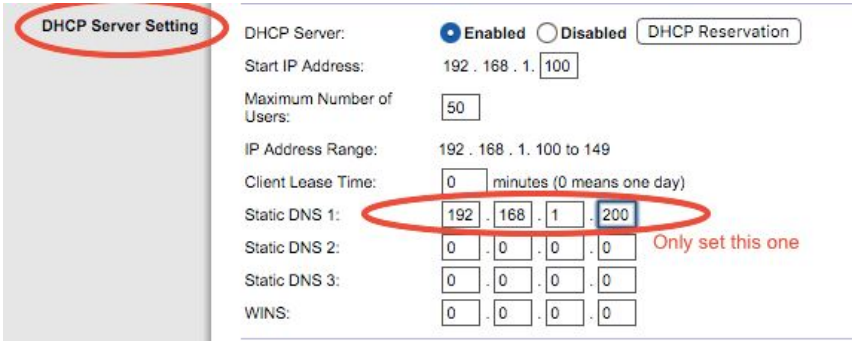
Pi-Hole

- open-source projekt síťového (doménového) filtru (aka. “DNS sinkhole”)
- aktivní vývoj od roku 2014, European Union Public Licence (EUPL)
- technologický stack
  - upravený dnsmasq (DNS+DHCP server)
  - webový server lighttpd
  - php (grafický web management)
- důraz na malé nároky na system (původně pro Raspberry Pi)
  - nyní jakýkoliv Linux
  - oficiální Docker image (vhodné i pro NAS)
- určený pro běh v lokální síti
  - vzdáleně přes Wireguard VPN (nutno dokonfigurovat)
  - umí lokální DNS zónu (např. .home, .internal)



Začínáme

- postup nasazení:
  - výběr platformy pro běh (Raspberry Pi, Linux kontejner, Docker, VPS,...)
  - instalace (shell skript s průvodcem), nebo Docker
  - základní nastavení (statická/dynamická IP adresa)
  - konfigurace zařízení v síti
    - DNS dotazy musí posílat na IP adresu Pi-Hole
    - nastavení DNS serverů na routeru:
  - Hotovo! A nebo ne?



Jak dále

- Rozhodně ne! Bez dalších **block listů** se neobejdete!
  - Block list je **seznam domén** který bude Pi-Hole blokovat
  - Pi-Hole block list nazývá “**Adlist**”
- volně dostupné na internetu
- tvořeny komunitně (dobrovolníci a cybersec firmy)
- kritéria pro vhodný block list:
  - uvedená kategorie: malware/phishing vs. reklamy/ad trackery
  - frekvence aktualizace
  - formát dat vhodný pro Pi-Hole
  - zdroj domén (ideálně tzv. primární zdroj)

Ukázka block listu

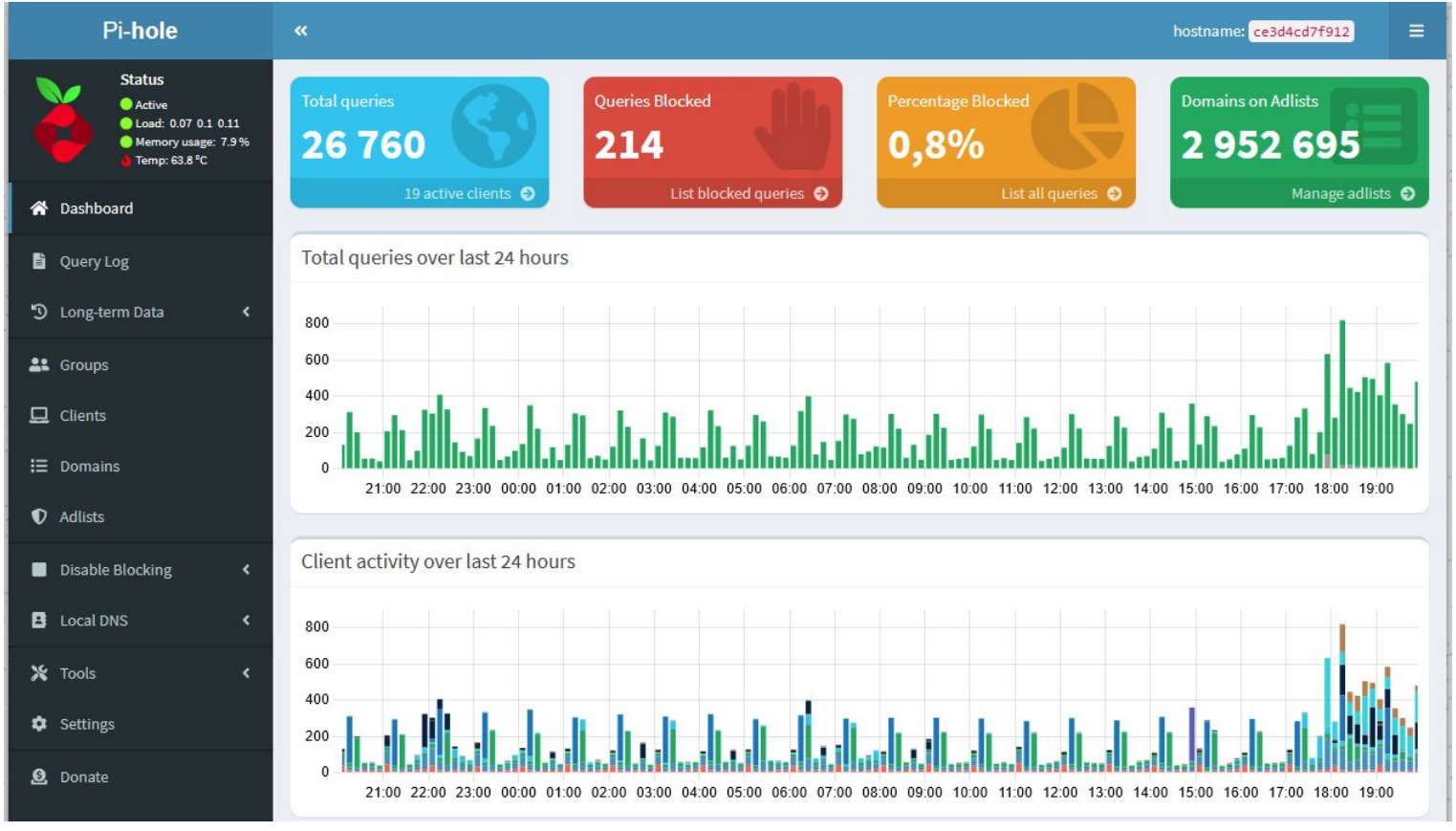
```
#
# Phishing Army | The Blocklist to filter Phishing
#
# Last Update: Thu, 24 Oct 2024 11:13:21 UTC
#
# Project website: https://phishing.army
# Support the project with a donation:: https://www.buymeacoffee.com/andreadraghetti
#
# This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
# ================================================================================================

0-01x-merchandise.554217.xyz
0-02pw.cfd
0-0llx.12313123.xyz
0-0lx.1231312.xyz
0-0lxmarket.5767435.xyz
0-0lxmarket.8796556.xyz
0-1x.8632152.xyz
0-2lyb.sbs
0-47pc.cfd
0-6n10.sbs
0-7l45.cfd
0-9m4v.sbs
0-a5e1.sbs
0-avn0.sbs
```

Block listy - best practice

- **pozor** na pokušení přidávat hromadně velké množství block listů najednou
  - hodnotu 10 kvalitních blocklistů zhatí jeden, který nebyl dostatečně zkontrolován
- dejte si čas na **vyhodnocení** nově přidaného block listu
  - některé zdroje mohou obsahovat např. zkracovače adres (např. bit.ly)
  - některé seznamy jen agregují jiné do jednoho velkého seznamu
  - pozor na blokování reklam a “ad trackerů” - ovlivní linky v reklamních emailech
- Pi-Hole aktualizuje block listy jednou za týden
  - většina block listů je aktualizovaná každých 24 hodin
  - lze upravit pomocí cronu

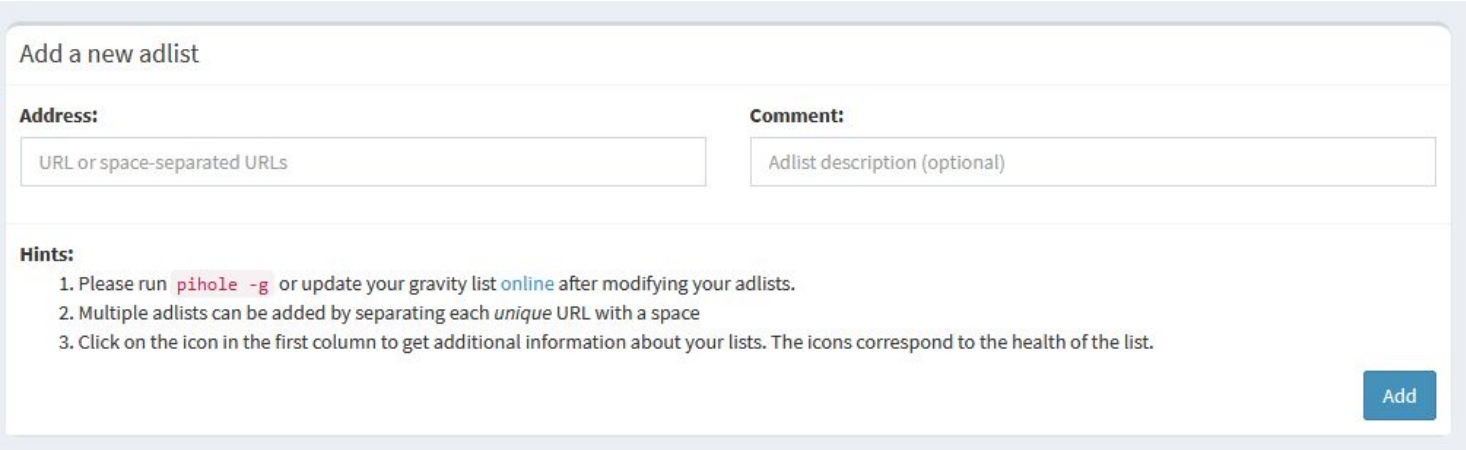
Ukázka webového rozhraní



Query log

2024-10-25 20:03:03	A	www.gstatic.com	ondra-del [redacted]	OK ([redacted]) INSECURE	IP (19.9ms)	Blacklist
2024-10-25 20:03:04	A	i.ytimg.com	ondra-del [redacted]	OK ([redacted]) INSECURE	IP (24.2ms)	Blacklist
2024-10-25 20:03:04	A	i.ytimg.com	ondra-del [redacted]	OK (cache) INSECURE	IP (0.2ms)	Blacklist
2024-10-25 20:03:04	AAAA	i.ytimg.com	ondra-del [redacted]	OK ([redacted]) INSECURE	IP (26.1ms)	Blacklist
2024-10-25 20:03:05	A	www.youtube.com	ondra-del [redacted]	OK ([redacted]) INSECURE	CNAME (25.9ms)	Blacklist
2024-10-25 20:03:05	A	youtube-ui.l.google.com	ondra-del [redacted]	OK (cache) INSECURE	IP (0.3ms)	Blacklist
2024-10-25 20:03:05	AAAA	youtube-ui.l.google.com	ondra-del [redacted]	OK ([redacted]) INSECURE	IP (18.1ms)	Blacklist
2024-10-25 20:03:07	A	jnn-pa.googleapis.com	ondra-del [redacted]	OK (answered by [redacted]) INSECURE	IP (21.8ms)	Blacklist

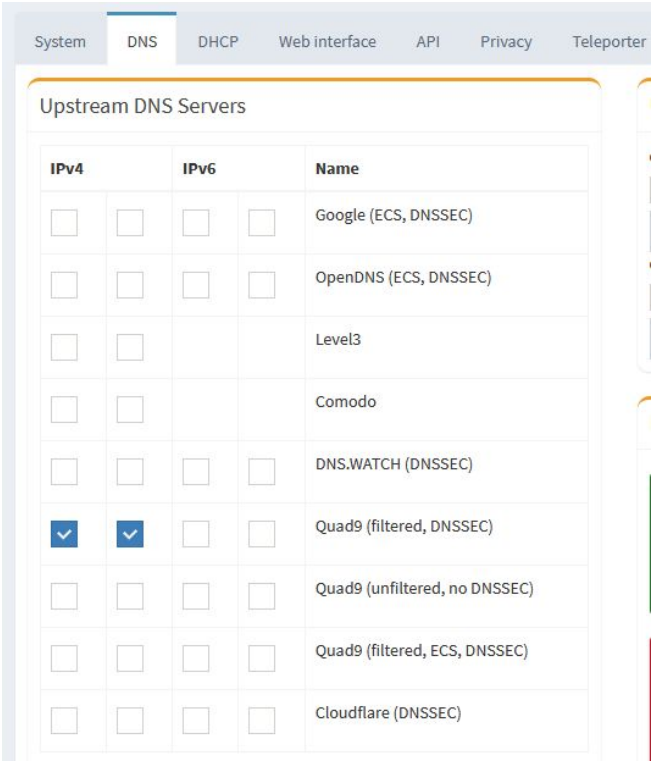
Správa block listů



	Address	Status	Comment	Group assignment	
☐	https://raw.githubusercontent.com/PolishFiltersTeam/KADhosts/master/KADhosts.txt	Enabled		Suspicious	
☐	https://someonewhocares.org/hosts/zero/hosts	Enabled		Suspicious	
☐	https://raw.githubusercontent.com/RooneyMcNibNug/pihole-stuff/master/SNAFU.txt	Enabled		Suspicious	
☐	https://v.firebog.net/hosts/AdguardDNS.txt	Disabled		Advertising	

Nastavení upstream serveru

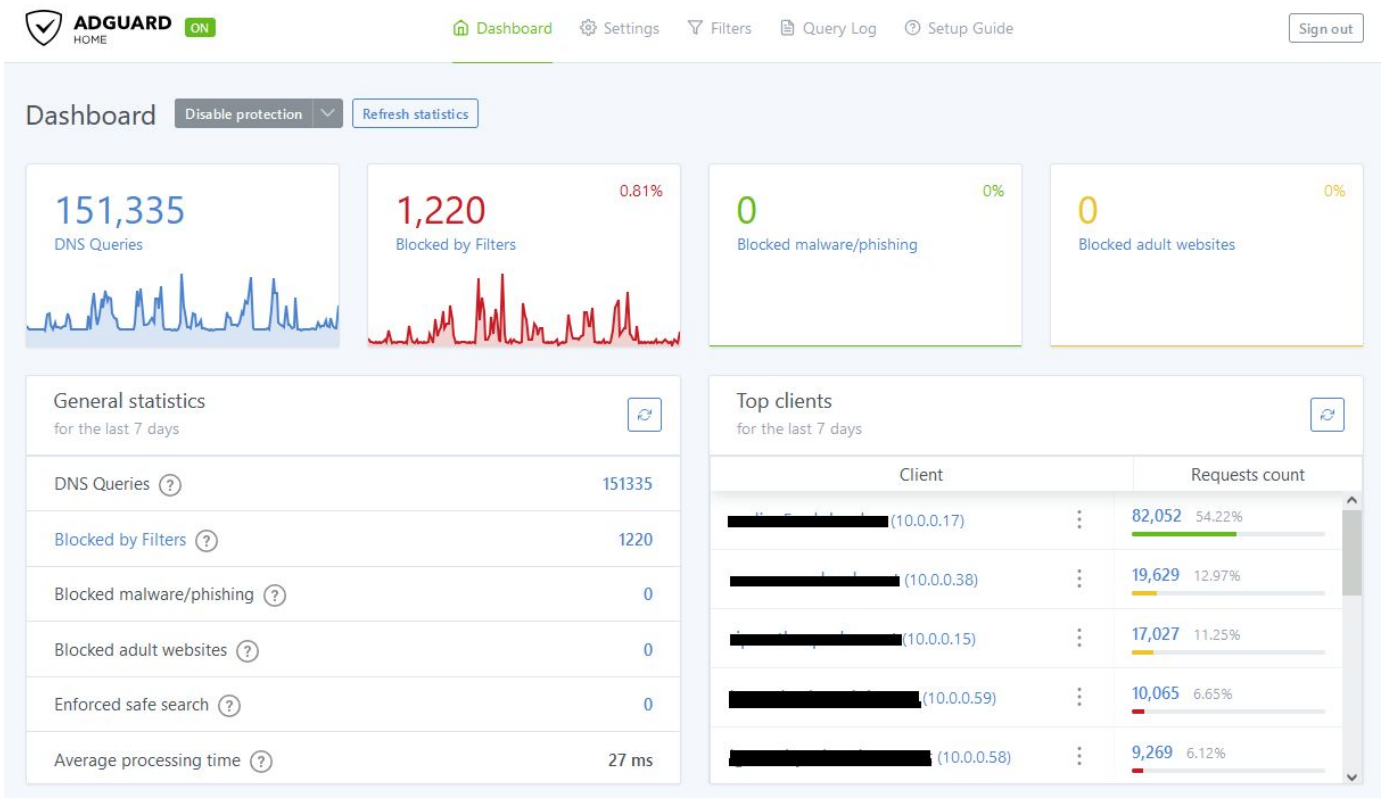
- Pi-Hole **neumí** sám rekurzivně vyhledávat domény
- potřebuje “nadřazený” DNS server který poskytne odpověď tzv. **upstream**
- pouze **nešifrovaný** DNS protokol
- Quad9 jako výchozí nastavení
- lze zvolit vlastní
  - např. i lokální (unbound)
  - DNS proxy podporující šifrování (např. CoreDNS)



AdGuard Home

- open-source DNS forwarder/filtr od Adguard Software Ltd.
- GPL-3.0 license, velmi aktivní vývoj (začátek 2018)
- technologický stack: Go, node.js, npm
- postup **nasazení** shodný s Pi-Hole
  - shell instalátor s průvodcem nebo docker image
- **podpora šifrovaných protokolů**
  - HTTTP pro webové rozhraní
  - DoH, DoT a DoQ
  - vhodné i pro vzdálený přístup (hosting na VPS)
- umí lokální DNS zónu (např. .home, .internal)

Webové rozhraní



Query log

21:58:03 25. 10. 2024	settings-win.data.microsoft.com Type: A, Plain DNS	Blocked PiHole - telemetry-windows	10.0.0.26 [redacted]	⋮
21:58:01 25. 10. 2024	slscr.update.microsoft.com Type: A, Plain DNS	Processed 37 ms	10.0.0.26 [redacted]	⋮
21:58:00 25. 10. 2024	fcmconnection.googleapis.com Type: A, Plain DNS	Processed 34 ms	10.0.0.26 [redacted]	⋮
21:58:00 25. 10. 2024	login.live.com Type: A, Plain DNS	Processed 43 ms	10.0.0.26 [redacted]	⋮
21:57:54 25. 10. 2024	accounts.google.com Type: AAAA, Plain DNS	Processed 63 ms	10.0.0.26 [redacted]	⋮
21:57:54 25. 10. 2024	accounts.google.com Type: A, Plain DNS	Processed 32 ms	10.0.0.26 [redacted]	⋮
21:57:41 25. 10. 2024	onclkds.com Type: A, Plain DNS	Blocked PiHole - Zero Hosts, PiHole - Anti Malw...	10.0.0.15 [redacted]	⋮

Správa block listů

DNS blocklists

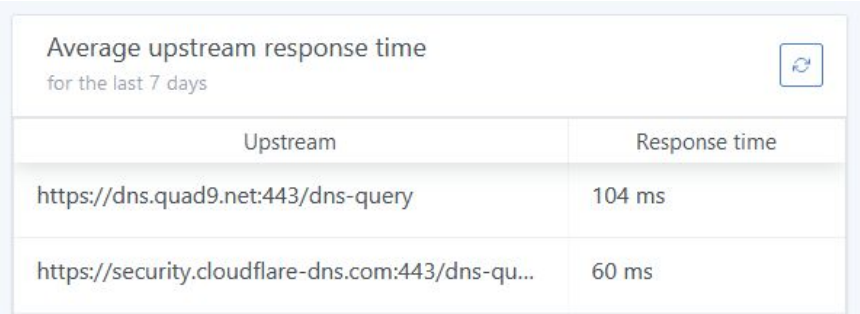
AdGuard Home will block domains matching the blocklists.

AdGuard Home understands basic adblock rules and hosts files syntax.

Enabled	Name	List URL	Rules count	Last time updated	Actions
✓	PiHole - Polish KADhosts	https://raw.githubusercontent....	80 059	25. října 2024 v 0:32	
✓	PiHole - Zero Hosts	https://someonewhocares.org/...	11 766	25. října 2024 v 0:32	
✓	PiHole - RooneyMcNibNug	https://raw.githubusercontent....	47 659	25. října 2024 v 0:32	
	PiHole - Adguard DNS	https://v.firebog.net/hosts/Ad...	0	10. října 2024 v 0:03	
✓	PiHole - Anti Malware Hosts	https://raw.githubusercontent....	25 797	25. října 2024 v 0:32	
✓	PiHole - Prigent Crypto	https://v.firebog.net/hosts/Pri...	16 282	25. října 2024 v 0:32	
✓	PiHole - Phishing Army	https://phishing.army/downlo...	245 743	25. října 2024 v 0:32	
✓	PiHole - Notrack Malware	https://gitlab.com/quidsup/no...	177	25. října 2024 v 0:32	

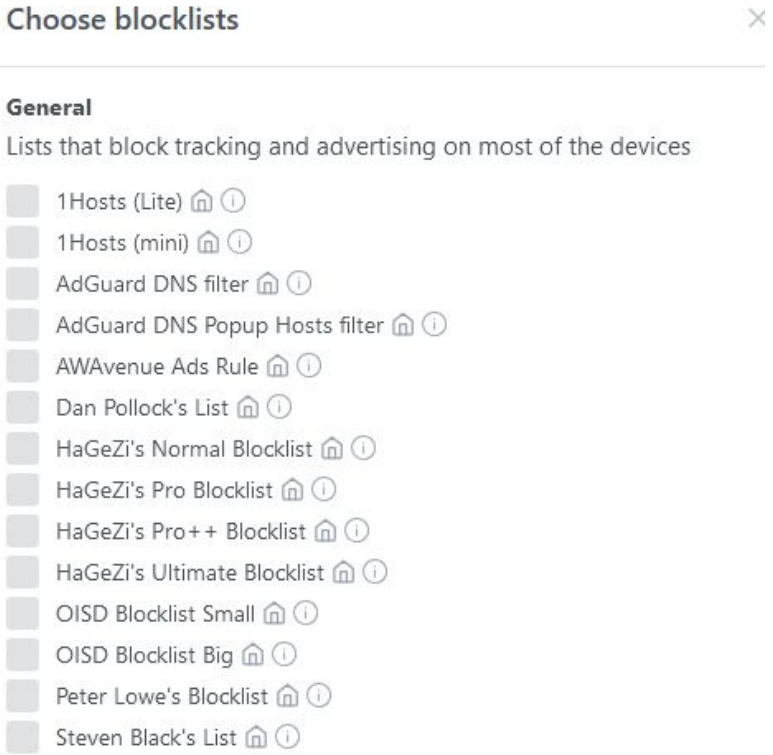
Nastavení upstream serveru

- AdGuard Home neumí sám rekurzivně vyhledávat domény
- potřebuje “nadřazený” DNS server který poskytne odpověď tzv. **upstream**
- podpora **šifrovaných** protokolů DoT a DoH
- možnost load balancingu, nastavení cache, timeoutu…
- seznam poskytovatelů: https://adguard-dns.io/kb/general/dns-providers/



Integrovaný seznam block listů

- velké množství přednastavených blocklistů
- odkaz na zdroj a popis včetně kategorií
- opět **pozor** na přidání mnoha blocklistů najednou
- možnost přidat i whitelisty
  - nutno sehnat z externího zdroje
  - pozor na kolizi s block listem



Srovnání

Funkce	AdGuard Home	Pi-Hole
Podporované platformy	Windows, macOS, Linux, Raspberry Pi, Docker	Linux, Raspberry Pi, Docker
DNS-over-HTTPS/TLS	**nativně**	vyžaduje nástroj 3. strany
Syntaxe filtrovacích pravidel	podpora komplexních pravidel	základní pravidla
Webové rozhraní	moderní	jednoduché ale funkční
Vestavěné filtry	**ano**	ne
Automatické aktualizace	ne	ano
Komunita	postupně rozrůstající	velká a stabilní

Zdroj: https://www.wundertech.net/adguard-home-vs-pi-hole-best-ad-blocker/

Cloud řešení

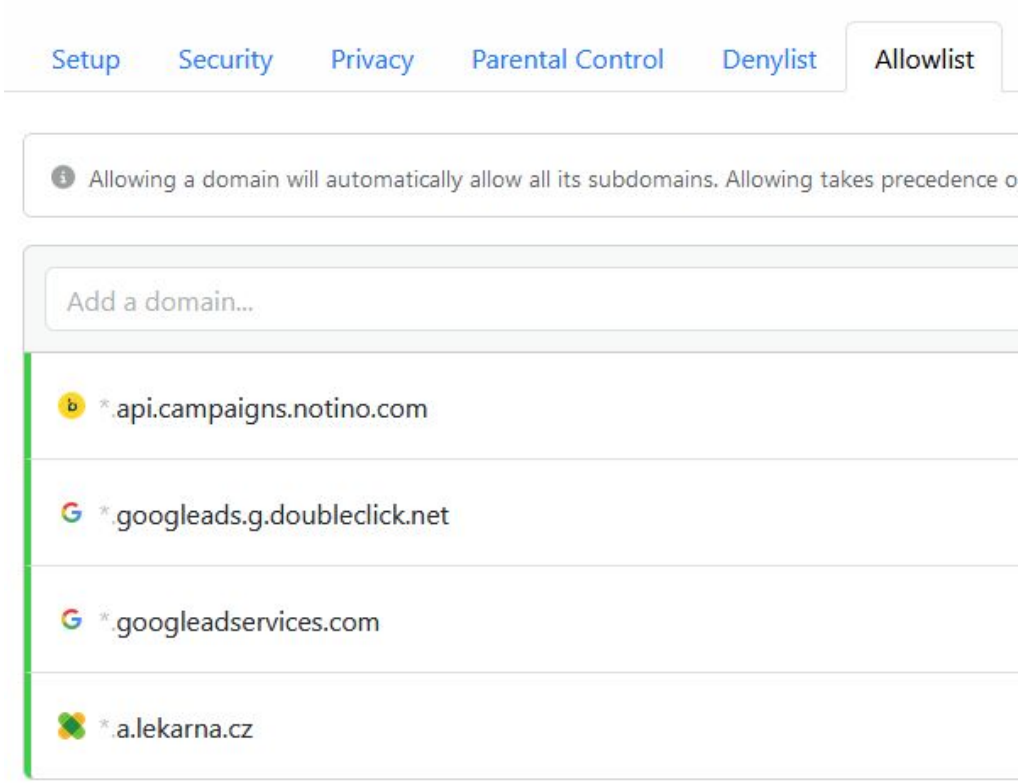
Cloud řešení

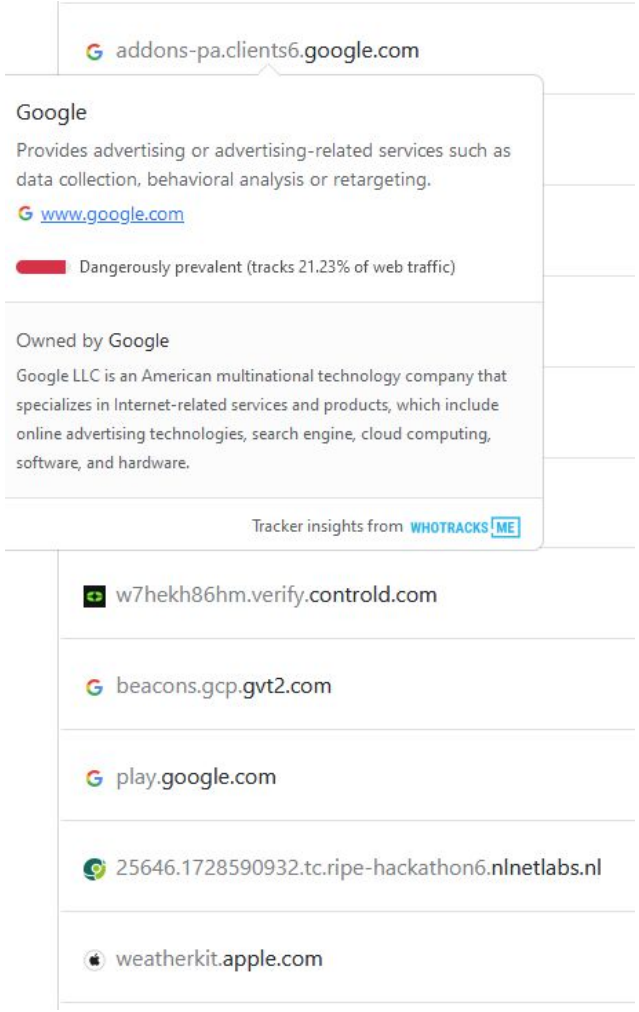
- pro uživatele kteří chtějí **něco navíc** oproti resolverům
- něco jako Pi-Hole/AdGuard Home, ale v cloudu
- nutná registrace a alespoň základní nastavení
- placená služba
  - často Free úroveň s omezením
- statistiky provozu s přehlednými grafy pro jednotlivá zařízení
- kontrola nad blokovanými kategoriemi
- vlastní (od)blokování jednotlivých domén
- důraz na soukromí
- příklady:
  - NextDNS (https://nextdns.io)
  - AdGuard DNS (https://adguard-dns.io)
  - ControlD (https://controld.com)

NextDNS

- všechny možné kombinace filtrů
  - security, privacy,
  - parental control
    - sociální sítě, 18+, gaming, ...
    - čas kdy je DNS funkční
    - anti-bypass (blokuje obcházení pomocí VPN)
- vlastní allow/deny listy
- detailní analýza provozu pro každého klienta
- podpora šifrovaných DNS protokolů
- široká podpora platforem, detailní návody pro koncová zařízení
- plán zdarma: 300 000 dotazů/měsíc

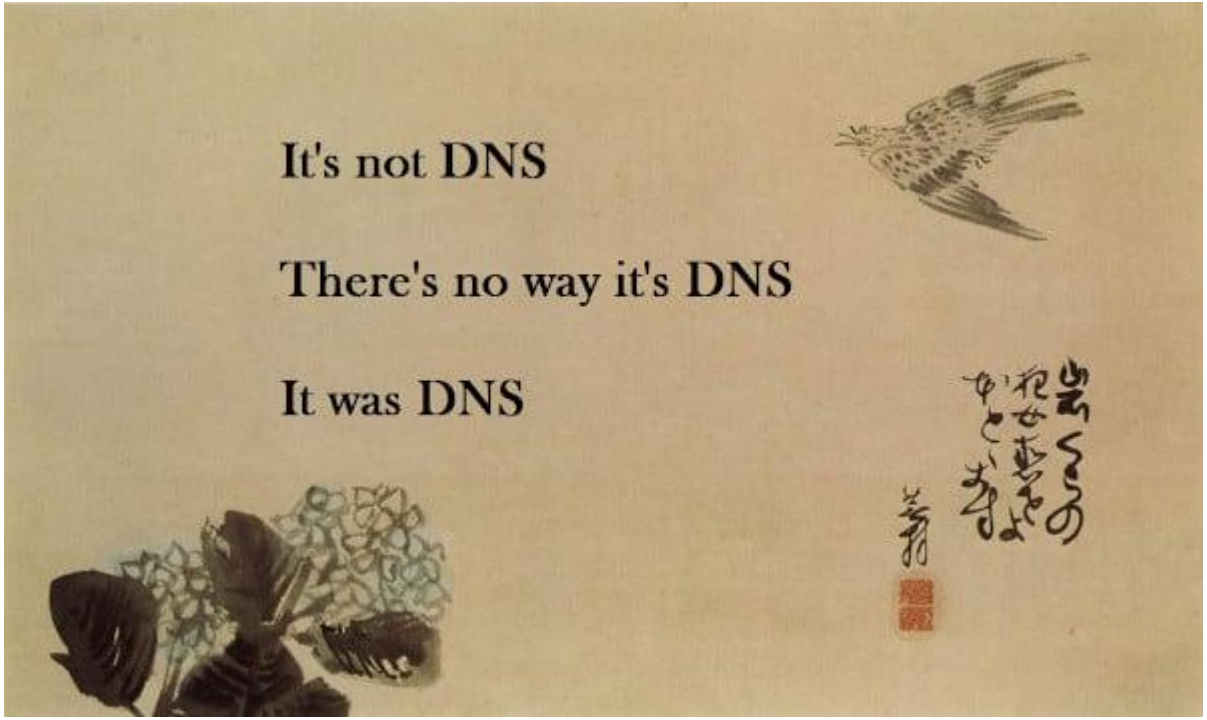
NextDNS


Setup
Security
Privacy
Parental Control
Denylist
Allowlist
Allowing a domain will automatically allow all its subdomains. Allowing takes precedence o
Add a domain...
*.api.campaigns.notino.com
*.googleads.g.doubleclick.net
*.googleadservices.com
*.a.lekarna.cz


addons-pa.clients6.google.com
Google
Provides advertising or advertising-related services such as data collection, behavioral analysis or retargeting.
www.google.com
Dangerously prevalent (tracks 21.23% of web traffic)
Owned by Google
Google LLC is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware.
Tracker insights from WHOTRACKS ME
w7hekh86hm.verify.controld.com
beacons.gcp.gvt2.com
play.google.com
25646.1728590932.tc.ripe-hackathon6.nlnetlabs.nl
weatherkit.apple.com

Závěr

- filtrování škodlivých domén **má smysl**
  - v konceptů kybernetické bezpečnosti je to **“hodně muziky za málo peněz”**
- přechod na bezpečné DNS je jednoduché a benefit je velký
- možností je více a vhodné pro každého
- více o soukromí a DNS:
  - https://www.privacyguides.org/en/dns/
  - https://dnsprivacy.org/


It's not DNS
There's no way it's DNS
It was DNS