

DNS-přes-???

Kdo a kam posílá DNS provoz?

Petr Špaček • petr.spacek@nic.cz • 28. 5. 2019



Základní rozdělení

- Nové transporty
 - DNS over TLS
 - DNS over HTTPS
 - QUIC?
- DNS v cloudu
- DNS v (každé) aplikaci
- Kombinace

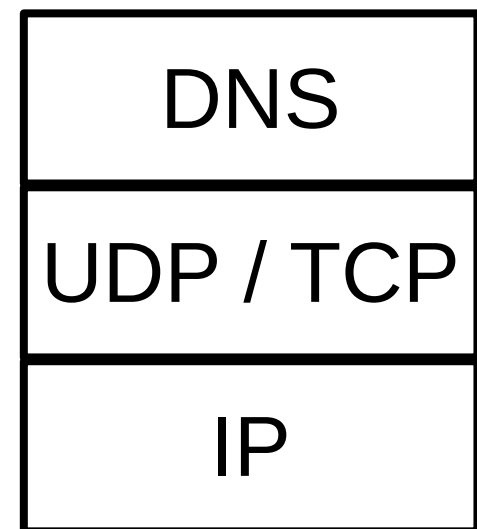


Transportní protokoly pro DNS



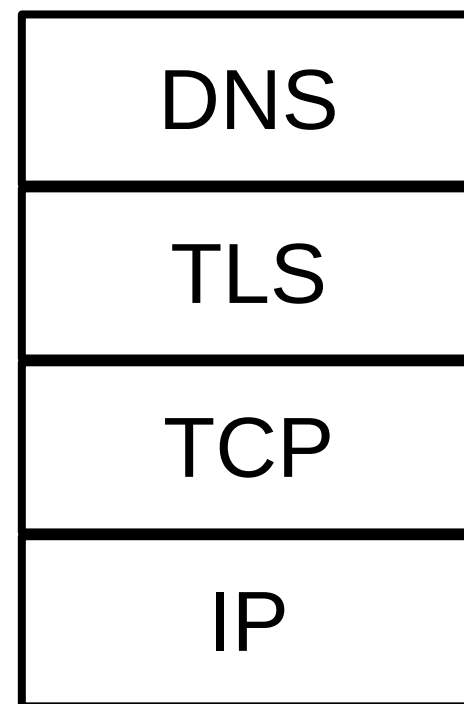
Klasické DNS

- UDP, TCP port 53
 - Lze snadno blokovat
 - Lze filtrovat
 - Bez autentizace serveru



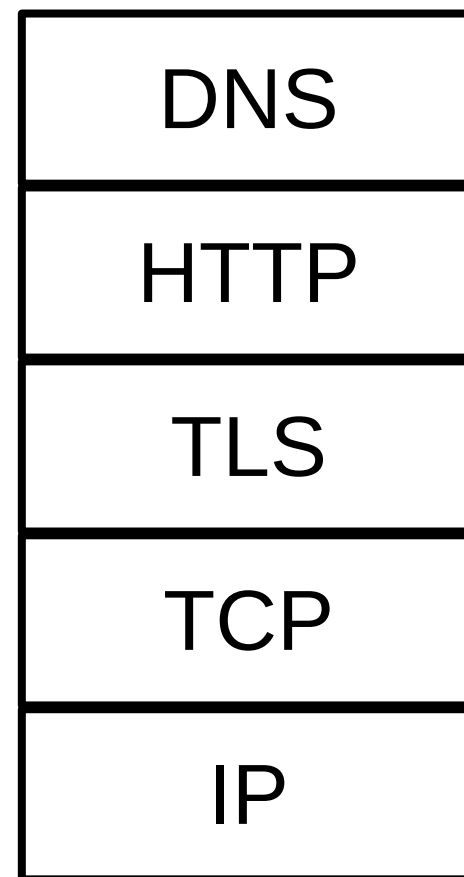
DNS over TLS = DoT

- DNS over TCP + obálka TLS
- TCP port 853
 - Lze snadno blokovat
 - Nelze číst ani modifikovat
 - Podporuje autentizaci serveru



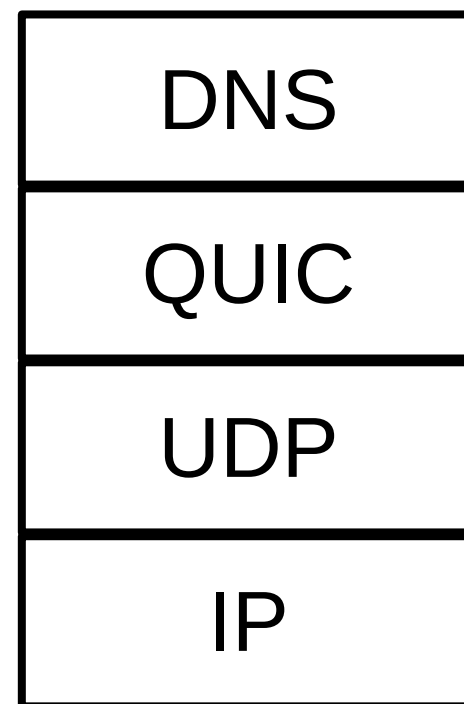
DNS over HTTPS = DoH

- DNS over UDP + obálka HTTP + TLS
- TCP port 443
 - Skrývá se v HTTPS provozu
 - Nelze snadno blokovat
 - Podporuje autentizaci serveru
- Rozdrobení jmenného prostoru



DNS over QUIC = DoQ?

- Prototypy bez standardu
- ???



Šifrované DNS: shrnutí

- **NEnahrazuje DNSSEC**
- Autentizace DNS resolveru
- Šifrování dat
- **Chybí auto-konfigurace**
- TLS SNI (Server Name Indication)
 - ESNi = Encrypted Server Name Indication
- Soukromí?
 - Plná VPN je lepší!



DNS v cloudu



DNS v cloudu

- Resolver mimo místní síť
- 1.1.1.1
- 8.8.8.8
- 9.9.9.9



DNS v cloudu: technické vlastnosti

- Ignoruje místní DNS
 - Split-horizon
 - Malware filter/RPZ
- Více provozu do Internetu
 - Datový tok ~ 10-30 krát
 - Počet TCP spojení ~ počet klientů/aplikací
- Latence?



DNS v cloudu: politika



- Jiná jurisdikce
 - Zákon 127/2005 § 97
Provozní údaje
... zejména údaje vedoucí k dohledání a identifikaci
zdroje a adresáta komunikace ...
 - GDPR
- Ignoruje místní (DNS) politiku
 - Zákon 186/2016 § 82
Blokace nepovolených internetových her



DNS v cloudu: implementace

- Dnes vyžaduje konfiguraci
- Zítra již nemusí ...
- "Opatření budou považována za dostatečná, pokud vedou k zabránění nebo alespoň ke ztížení přístupu k internetovým stránkám uvedeným na Seznamu a ke skutečnému odrazování uživatelů internetu od účasti na nelegálních hazardních hrách alespoň takovým způsobem, **že uživatel vědomě překonává opatření** stanovená českým právním řádem ..."

DNS v aplikacích



DNS "tradičně"

- Aplikace
- DNS knihovna operačního systému
- Lokální resolver (z DHCP)



DNS v aplikaci

- Aplikace
- Knihovna OS
- Lokální resolver

- Aplikace
- ~~Knihovna OS~~
- Lokální resolver(y)

- Cache
- Split-horizon
- Filtrování?



DNS v (každé) aplikaci

- Firefox
- ~~Knihovna OS~~
- Resolver 1.1.1.1
- Outlook
- Knihovna OS
- Lokální resolver
- Chrome
- ~~Knihovna OS~~
- Resolver 8.8.8.8
- YouTube
- Knihovna OS
- Resolver 8.8.8.8



Vítězem se stává ...



Trusted Recursive Resolver (TRR)



A dramatic night sky with multiple bright lightning bolts striking down towards a city skyline. The lightning bolts are jagged and bright white/yellow, contrasting sharply with the dark blue night sky. The city lights at the bottom are blurred and warm, providing a base for the intense light of the lightning.

Co to znamená?

Dopady: DNS v cloudu

- Nárůst provozu
 - Odhad 10 – 30 x šířka pásma
 - Nárůst počtu TCP spojení
- ISP content cache
 - EDNS client subnet
 - Posílá podsít' klienta do Internetu
 - Nově závisí na Cloud resolveru



Dopady: DNS v aplikacích

- Noční můra technické podpory
- Tříští konfiguraci
- Kde je cache?
- Kdo a kam posílá dotazy?
 - Split-horizon? Lokální tiskárna?
 - Filtry?



Dopady: Šifrované DNS v aplikacích

- Noční můra bezpečáků
- RPZ není použitelné
- Skrývání C&C domén
- Těžší monitoring malware



Dopady: Cloud

- Noční můra právníků
- Jaké regulace se aplikují a na koho?
 - Ustoupí MF ČR Mozille?
- GDPR, Cloud, Snowden v USA

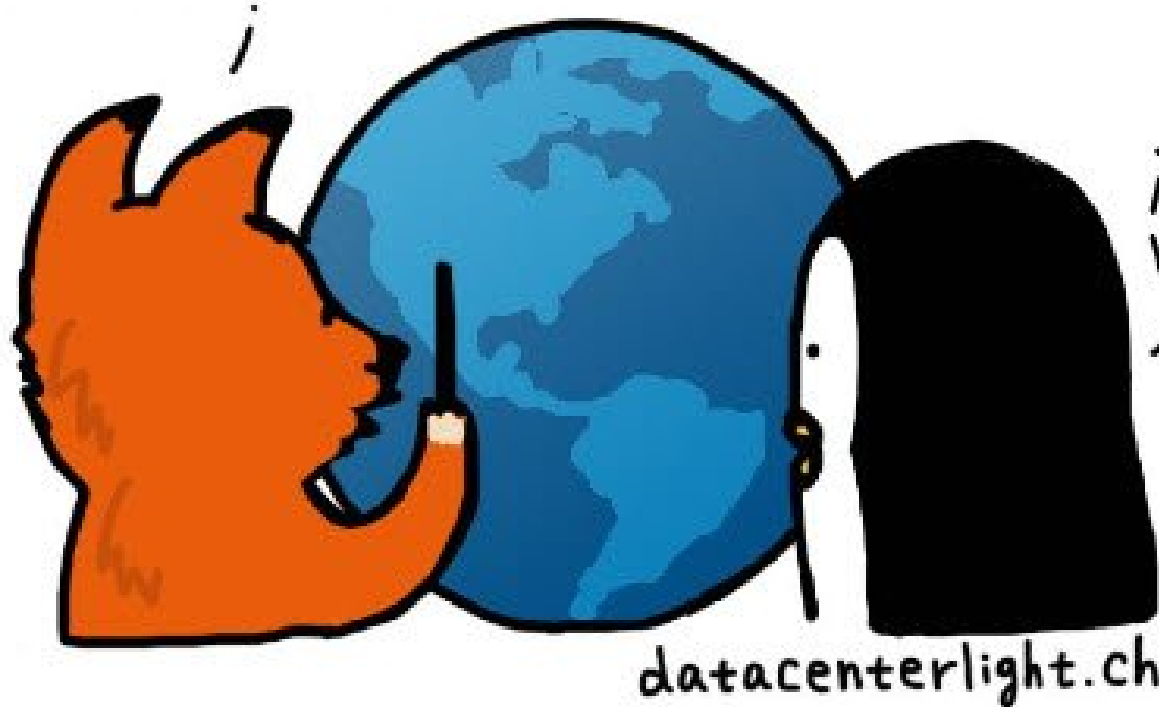


Dopady: Šifrování + Cloud + Aplikace

- **Soukromí?**
- Ztížení on-path sledování
- **ALE!** Menší granularita sledování pro resolver
- Resolver: domácnost -> zařízení -> aplikace
- Autoritativní strana: ISP -> Client subnet
- Potenciální centralizace

Firefox TRR aneb ...

ALL YOUR DATA WILL BE SAFE.
IT WILL BE JUST BETWEEN
ME AND YOU. OH AND THIS COMPANY
OVER HERE WHO'S GONNA MAKE
SURE IT'S GONNA BE SAFE.



...I THINK JUST
ME AND YOU
WAS SAFER.



Co dál?

- Šifrované transporty k ISP DNS resolveru?
- Zveřejnění zásad ochrany údajů
- "Slušné" chování
 - <https://wiki.mozilla.org/Security/DOH-resolver-policy>
- Moderní resolvers jsou k dispozici



Prostor pro diskusi

- <https://www.ietf.org/mailman/listinfo/add>
- add@ietf.org

Děkuji za pozornost!

