# Soukromí v DNS

## Novinky z IETF

Ondřej Surý • ondrej.sury@nic.cz • 03. 12. 2016

# Pracovní skupina **dprive** (DNS Privacy Exchange)

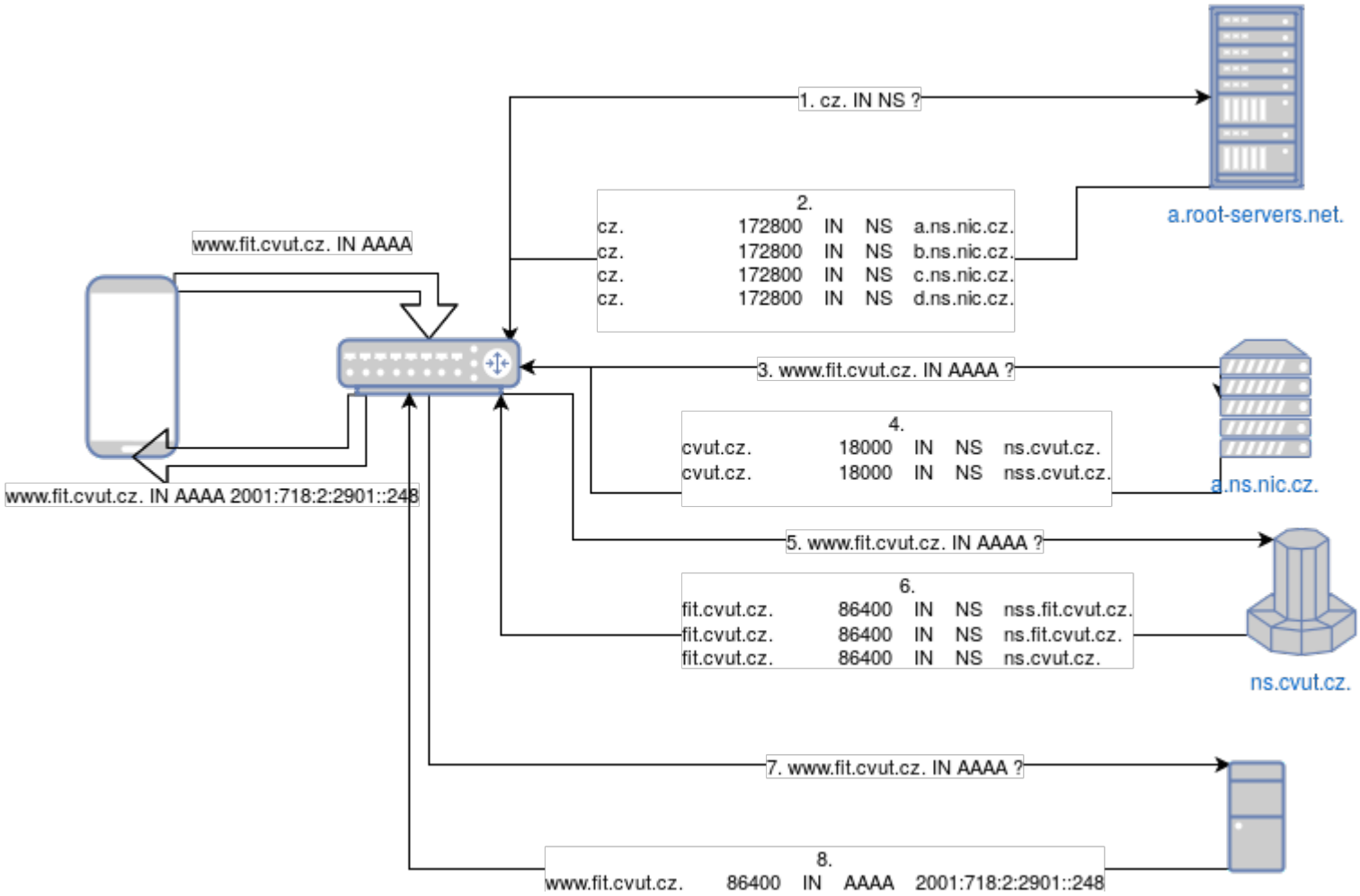
## Standardy

- RFC7816: QNAME Minimization
- RFC7858: DNS over TLS (TCP)
- RFC7830: EDNS0 Padding

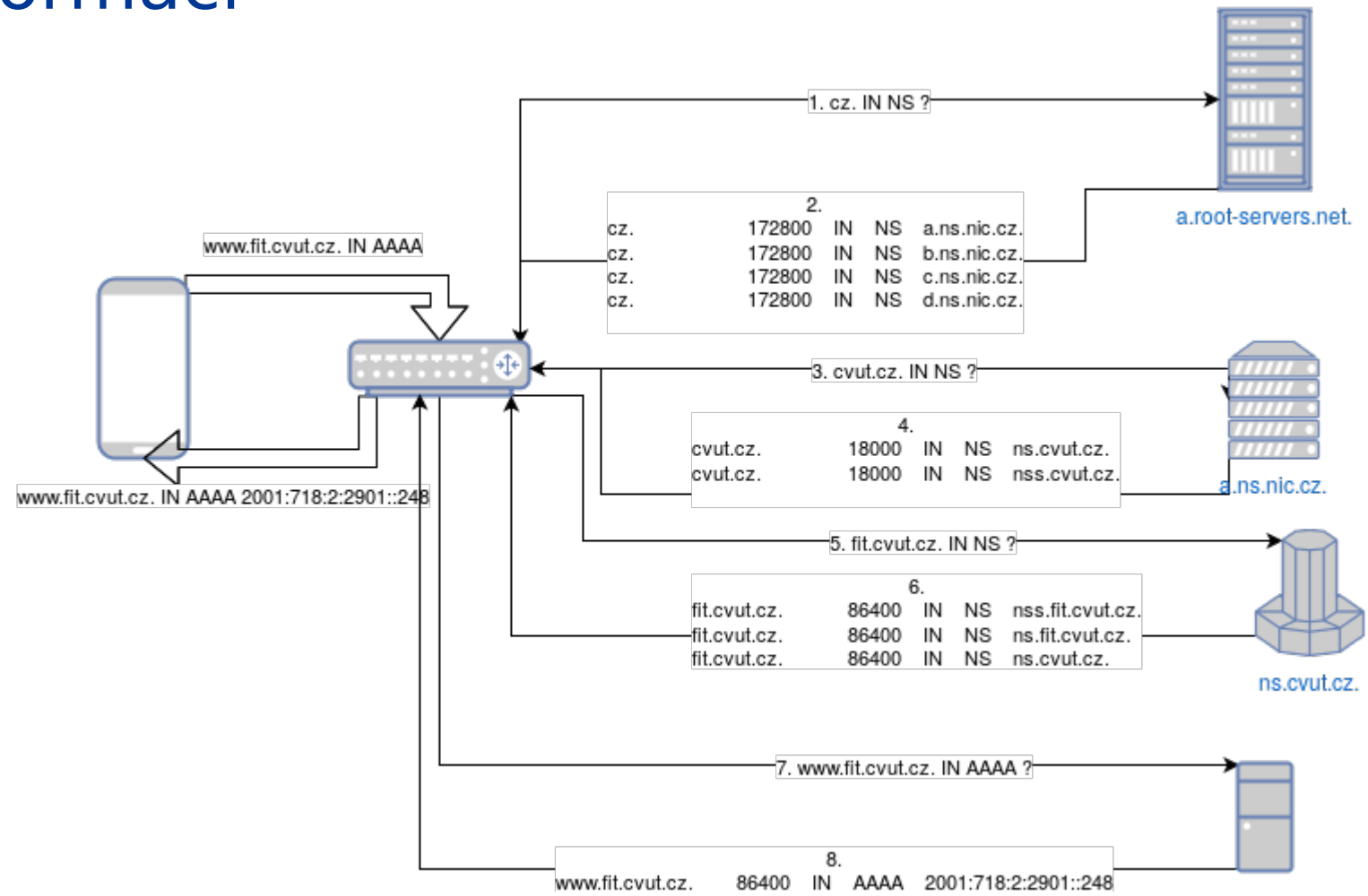
## Internetové drafty

- DNS over DTLS
- Authentication and (D)TLS Profile for DNS-over-(D)TLS
- Padding Profiles for EDNS(0)

# QNAME Minimization – Klasické DNS



# QNAME Minimization – minimalizace informací



# QNAME Minimization

- Předáváme minimum potřebných informací
- Kdy zastavit minimizaci?
  - Ve chvíli, kdy jsme iterovali přes všechny labely
    - DoS vektor (a.b.c.d.e.f.g.h.....)
    - IPv6
    - => Omezený počet iterací
  - Pokud dostaneme jiný RCODE než NOERROR
    - NXDOMAIN
      - www.whitehouse.gov -> gov.edgekey.net. IN NS -> NXDOMAIN
      - RFC8020: NXDOMAIN: There Really Is Nothing Underneath
    - REFUSED
    - SERVFAIL
    - => Možnost “úteku”

# QNAME Minimization – Test

$ kdig IN TXT qnamemintest.internet.nl.

QNAME Minimization zapnuta:

"HOORAY - QNAME minimisation is enabled on your resolver :)!"

QNAME Minimization vypnuta:

"NO - QNAME minimisation is NOT enabled on your resolver :("

Stav implementací

Knot Resolver – standardně zapnuto

Unbound – standardně vypnuto

BIND – 9.12?

PowerDNS Recursor – 4.1.0?

# DNS over TLS

- Zabezpečení kanálu mezi:
  - stub (koncovým klientem) a rekurzivním serverem
  - stub a forwardujícím serverem
  - forwardujícím a rekurzivním serverem
- Přidělen port **853**
  - Kvůli deep packet inspection
  - Catchall firewally (hotelové sítě)
- Klasické TLS (1.x)
- Volitelné ověření druhé strany (draft-ietf-dprive-dtls-and-tls-profiles)
  - Oportunistické (když je, tak je)
  - Striktní
    - PKIX

# DNS over TLS – Stav implementací

## Serverová strana

- Knot Resolver
- Unbound
- Libovolný DNS server s TLS Proxy
  - Nginx
  - HAProxy
  - stunnel
- https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+test+servers

## Klientská strana

- Knot DNS kdig
- drill (ldns)
- digit (https://ant.isi.edu/software/tdns/digit/index.html)
- getdns (http://getdnsapi.net/)

# DNS over TLS vs DNS over DTLS

- DNS over TLS (TCP)
  - Navázaní spojení
    - TCP handshake
    - TLS handshake
  - Obnovení spojení (session resumption)
    - TCP handshake
- DNS over DTLS (UDP)
  - Navázaní spojení
    - (D)TLS handshake
  - Obnova spojení
    - 1 round trip
- TCP Fast Open [RFC7413]

# EDNS0 Padding

- Metadata v případě DNS prozradit informace
  - kratka.cz vs velmidlouhadomena.cz
  - Délka dotazu
  - Délka odpovědi
- EDNS0 Padding přidává data do DNS zprávy
- Rozšíření pro DNS over TLS
  - Použití pouze v šifrovaném kanálu
  - V nešifrovaném to nedává smysl
- Padding strategie (draft-mayrhofer-dprive-padding-profile):
  - No padding
  - Fixní délka
  - Zarovnání do bloku

# EDNS0 Padding – Stav implementací

- Serverová strana:
  - Knot Resolver
- Klientská strana
  - Knot DNS kdig
  - getdns

# Otázky? Vajíčka? Rajčata?

Ondřej Surý • ondrej.sury@nic.cz • 03. 12. 2016