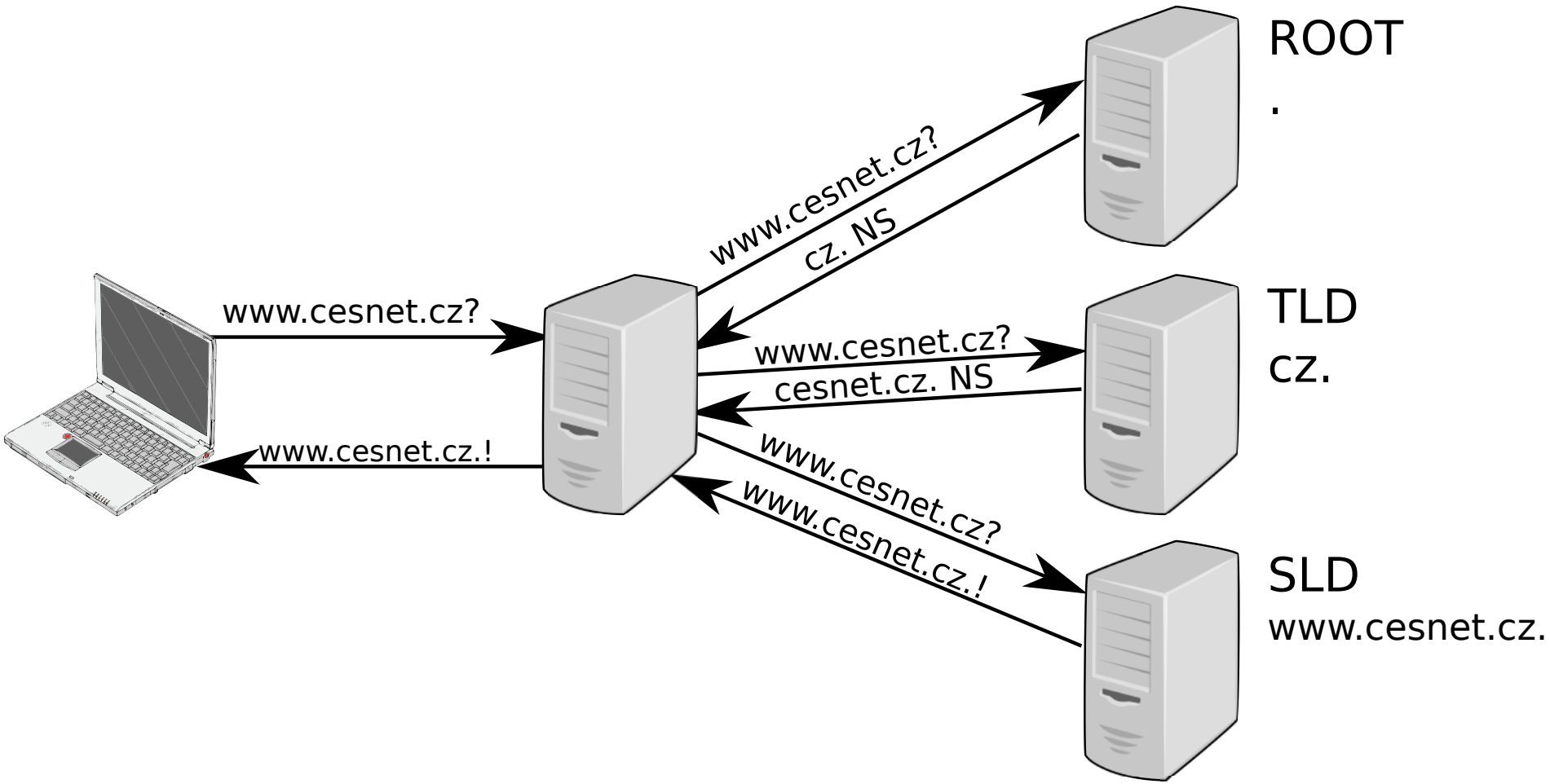
Provozování DNS

Ondřej Caletka

4. února 2014

Obsah

O službě DNS


ROOT
.
TLD
cz.
SLD
www.cesnet.cz.
www.cesnet.cz?
cz. NS
www.cesnet.cz?
www.cesnet.cz?
cesnet.cz. NS
www.cesnet.cz?
www.cesnet.cz.!
www.cesnet.cz.!
stub resolver
rekurzivní resolver
autoritativní server

Tři druhy DNS nodů

stub resolver knihovní funkce operačního systému

- s minimální cache
- v GNU C knihovně nepříliš robustní

rekurzivní resolver řeší dotazy a kešuje odpovědi

- agresivní cache řízená TTL hodnotami
- validace DNSSEC dat
- robustní řešení nedostupnosti autoritativních serverů

autoritativní server poskytuje data

- pouze ta, která má v databázi

CESNET

Rekurzivní servery

- malá diverzita v implemetacích:
  - BIND
  - Unbound
  - *PowerDNS recursor* − neumí DNSSEC
  - *Dnsmasq* je ve skutečnosti jen *forwarder*
- nutno zapnout ručně validaci DNSSEC
  dělají to velcí operátoři, není se čeho bát
- nutno omezit povolené IP adresy pro dotazy
  a implementovat BCP 38 ve své síti

Problém řetězení resolverů s DNSSEC

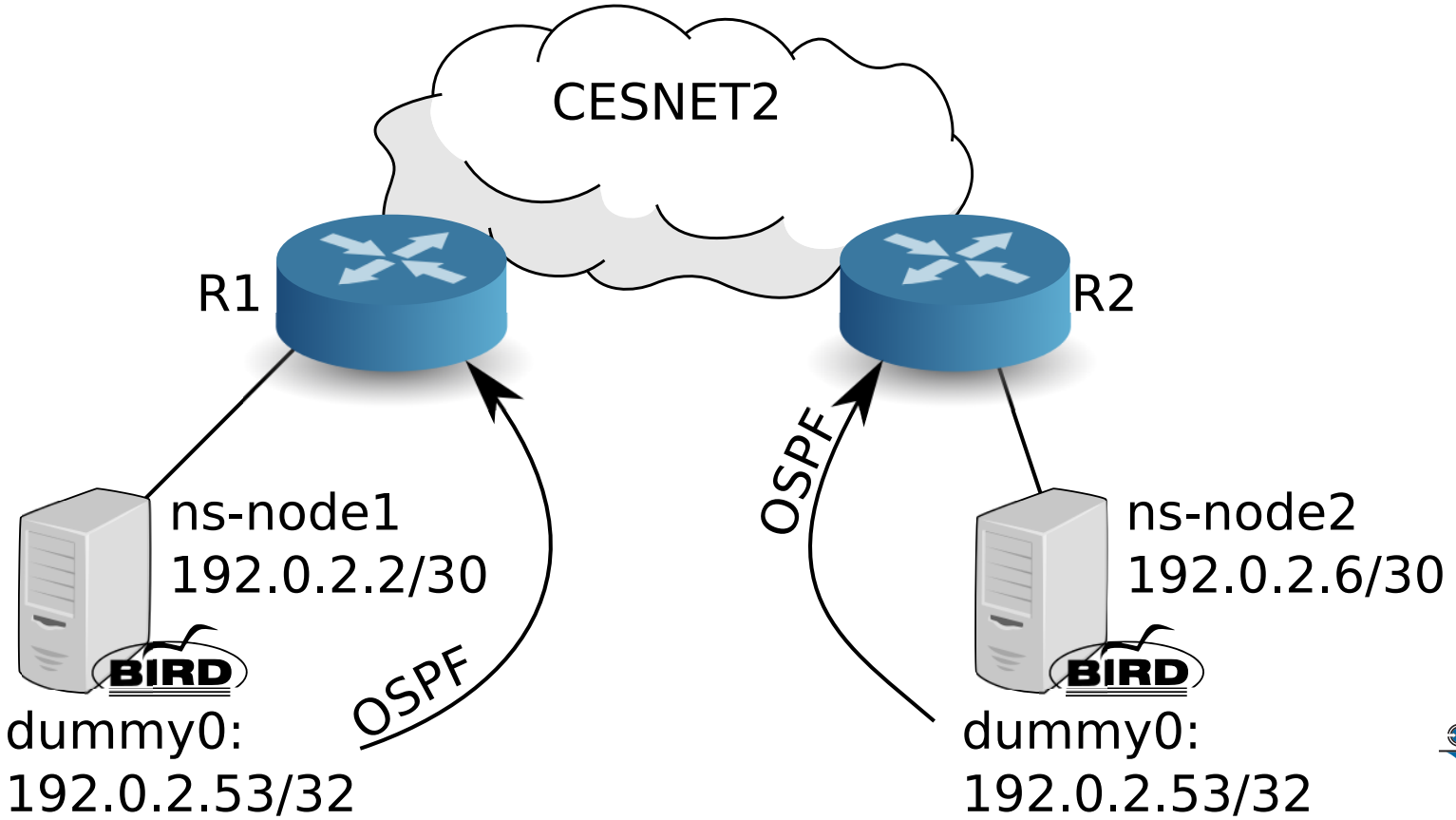
- problematická validace žolíkových domén
- zejména, je-li forwardováno na BIND
- automatizovaný test na `http://wildcarddnssec.jdem.cz/`

Test		Výsledek testu
1.	Zabezpečení DNSSEC *.wilda.rhybar.0skar.cz	Úspěch. Nedostanete se na doménová jména s neplatným podpisem.
2a.	NSEC zóna s A záznamem *.wilda.nsec.0skar.cz	Neúspěch. Váš DNS server nedokáže správně validovat *A záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC.
2b.	NSEC zóna s CNAME záznamem *.wild.nsec.0skar.cz	Neúspěch. Váš DNS server nedokáže správně validovat *CNAME záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC.
3a.	NSEC3 zóna s A záznamem *.wilda.0skar.cz	Neúspěch. Váš DNS server nedokáže správně validovat *A záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
3b.	NSEC3 zóna s CNAME záznamem *.wild.0skar.cz	Neúspěch. Váš DNS server nedokáže správně validovat *CNAME záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
4.	NSEC s extra záznamem uvnitř žolíku www.wilda.nsec.0skar.cz	Úspěch. Váš DNS server správně validuje *CNAME záznam*, obklopený žolíkovými *A záznamy* na zóně s NSEC.
5.	NSEC3 s extra záznamem uvnitř žolíku www.wilda.0skar.cz	Úspěch. Váš DNS server správně validuje *CNAME záznam*, obklopený žolíkovými *A záznamy* na zóně s NSEC3.

Vysoká dostupnost rekurzivních serverů

hodí se zejména v kombinaci s GNU stub resolverem

- tradiční HA pomocí linux-HA, pacemaker…
- anycasting v rámci vlastní sítě
  zabezpečí i proti výpadku routeru



Autoritativní servery

Mnoho slušných implemetací:

- BIND
- NSD
- Knot DNS
- *YADIFA*
- *PowerDNS*

Klíčové vlastnosti:

- podpora DNSSEC včetně NSEC3
- podpora dynamického DNS
- (ne-)podpora kombinace autoritativního a rekurzivního serveru

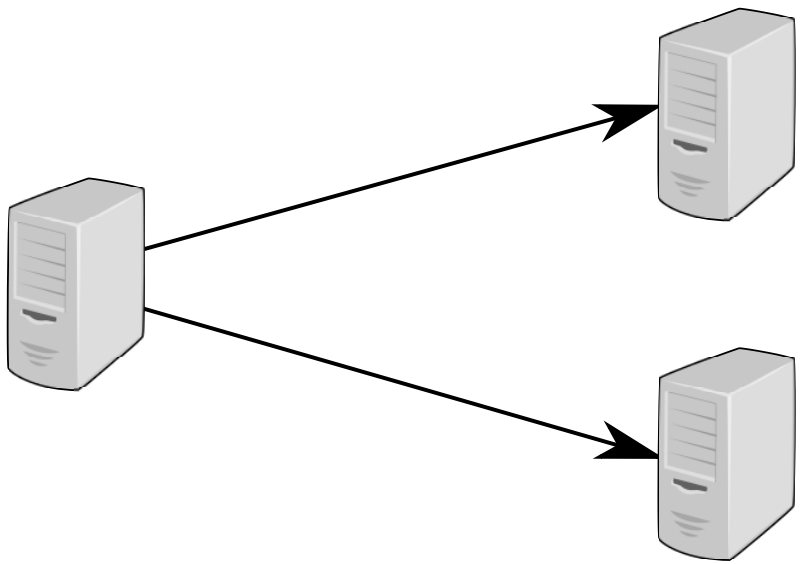
DNSSEC na autoritativních serverech

Možné přístupy:

1. online podepisování
   - DNS server drží privátní klíče
   - podepisuje buď po načtení, nebo v reakci na dotaz
   - snadná spolupráce s dynamic DNS
   - možné problémy s přenosem na sekundární servery
2. externí podepisování
   - DNS server má k dispozici zónu včetně předem vytvořených podpisů
   - privátní klíče jsou potřeba pouze při změně dat
   - hotové produkty jako OpenDNSSEC

Zónové přenosy

- úplné (AXFR) a inkrementální (IXFR)
- rychlé notifikace zprávami NOTIFY
- ochrana celistvosti zpráv pomocí TSIG
- nutno zvyšovat sériové číslo zóny
- princip skrytý master – veřejný slave



hidden master public slave

Časování a synchronizace

- odpovědi serverů kešovány po TTL daného záznamu
- negativní odpovědi kešovány podle hodnoty `SOA minimum`
- nesynchronnost serverů vede ke *split-brain*:
  o odpovědi rozhoduje náhoda

Za jak dlouho se změna nejpozději projeví?

	s `NOTIFY`	bez `NOTIFY`
nový	`SOA minimum`	`SOA minimum + SOA refresh`
změna	`TTL starého`	`TTL starého + SOA refresh`

Proč nepoužívat obskurní DNS servery

```
$ host www.skvelabanka.cz
www.skvelabanka.cz has address 192.0.2.7
Host www.skvelabanka.cz not found: 3(NXDOMAIN)

$ host www.skvelabanka.cz
Host www.skvelabanka.cz not found: 3(NXDOMAIN)
```

- programátor nepředpokládal, že se někdo zeptá na MX záznam pro www.skvelabanka.cz
- jeho implementace na takový dotaz vracela NXDOMAIN s TTL = 1 hodina
- BIND takovou odpověd nakešoval a po dobu TTL nevracel žádná data pro www.skvelabanka.cz

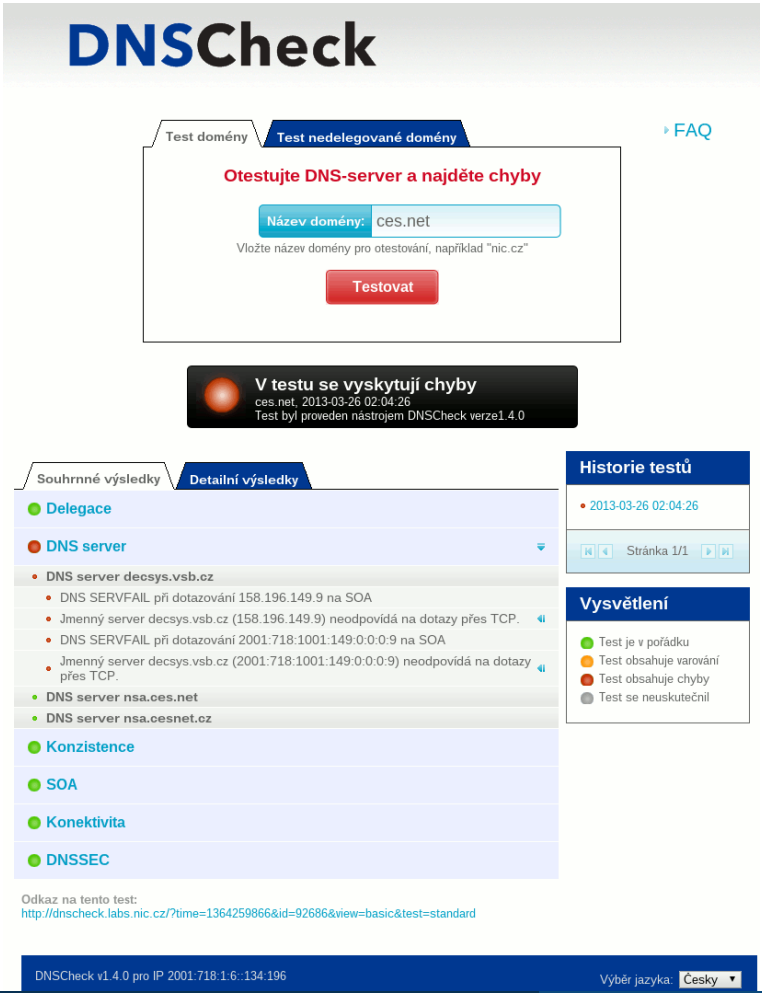
Proč nekombinovat autoritativní a rekurzivní server na jedné IP adrese

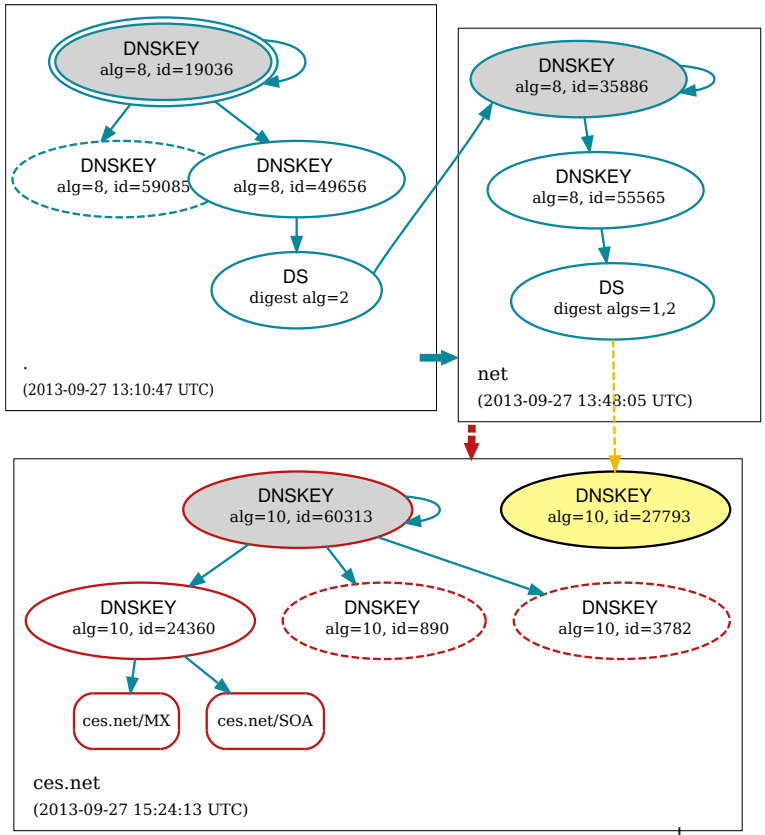
- malá škála dostupného DNS software (BIND a PowerDNS - ale bez DNSSEC)
- nemožnost DNSSEC validace vlastních dat (data z disku se nikdy nevalidují)
- špatná data z oddelegovaných, ale nezrušených zón

„Veškerá pošta nám už chodí na nový server, kromě pošty od našeho bývalého registrátora. Ta chodí stále na starý server.“

On-line kontroly

- http://dnsviz.net
- http://dnscheck.labs.nic.cz





Pravidelné údržby DNS serverů

- kontrola, že jsou zóny stále nadelegovány
- kontrola shody delegace s NS záznamy v zóně

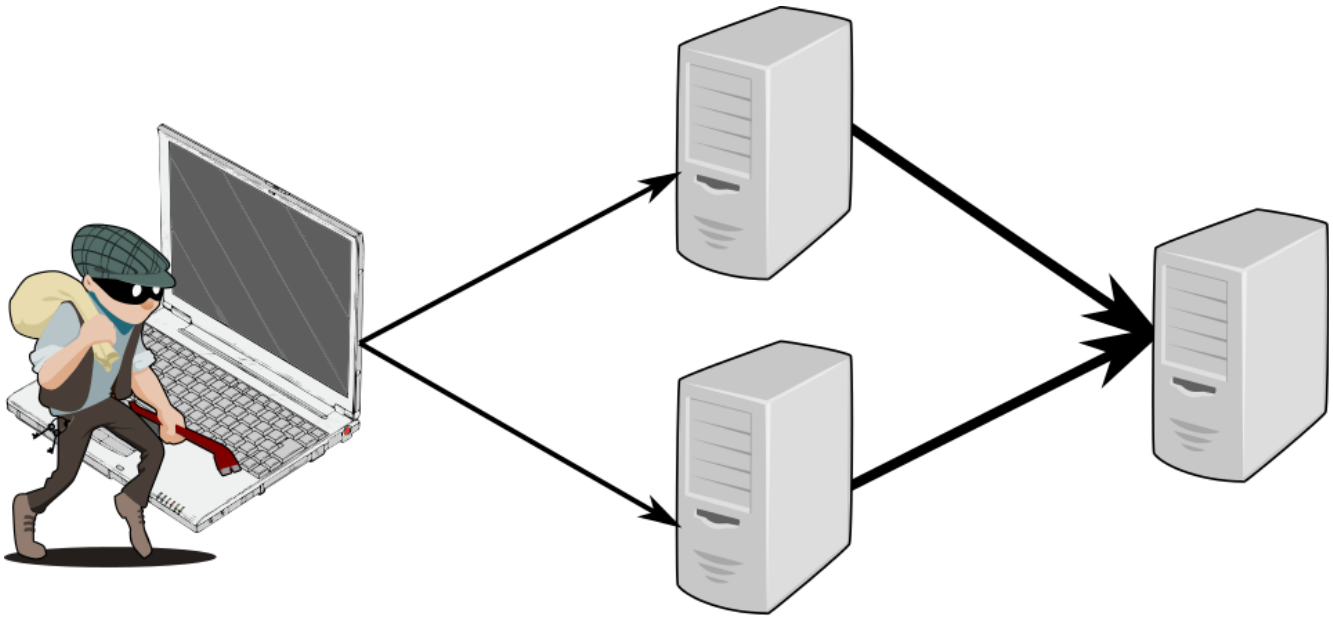
Vlastní řešení `http://ldnshealth.jdem.cz`

```
xargs ./dnsservercheck.py server.example.com < list_of_domains.txt
example.cz: server server.example.com. not in delegation nor zone apex
example.com: server server.example.com. delegated, but not in zone apex
example.net: server server.example.com. not in delegation nor zone apex

List of domains, which should be deleted from server config:
example.cz
example.net
```

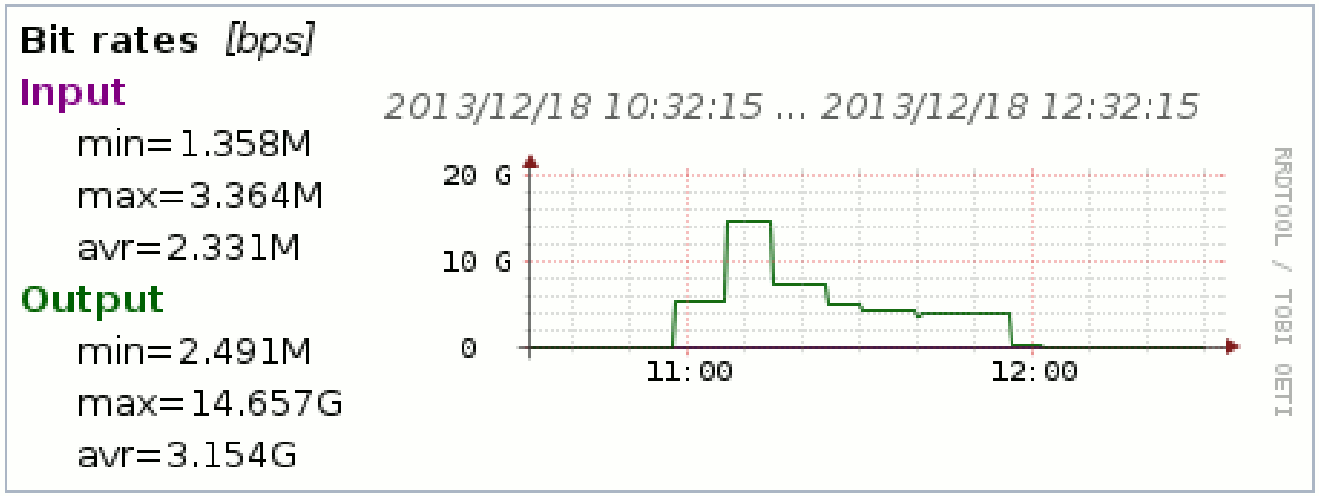
Útoky na/pomocí DNS

- odepření služby rekurzivního serveru
- zesilující útok odrazem od DNS serverů



Odepření služby zahlcením

- incident 18. 12. 2013 11:00 – 12:00 CET
- zahlcení hlavního DNS resolveru UDP pakety na náhodná čísla portů, *obsahující 128 × 0x00*
- provoz přicházel ze všech zahraničních linek z náhodných adres
- možné protiopatření: ACL na hraničních routerech



Potírání zesilujících útoků

- implementujte BCP 38 (a nuťte ostatní)
- neotvírejte rekurzivní servery do světa
  a zkontrolujte taky NTP servery a zařízení se SNMP ☺
- na autoritativních serverech zapněte RRL

Response Rate Limiting

Obecná technika limitování odpovědí autoritativních serverů na opakující se dotazů ze stejné adresy. Implementováno nativně v Knot DNS a NSD, existují patche pro BIND 9.

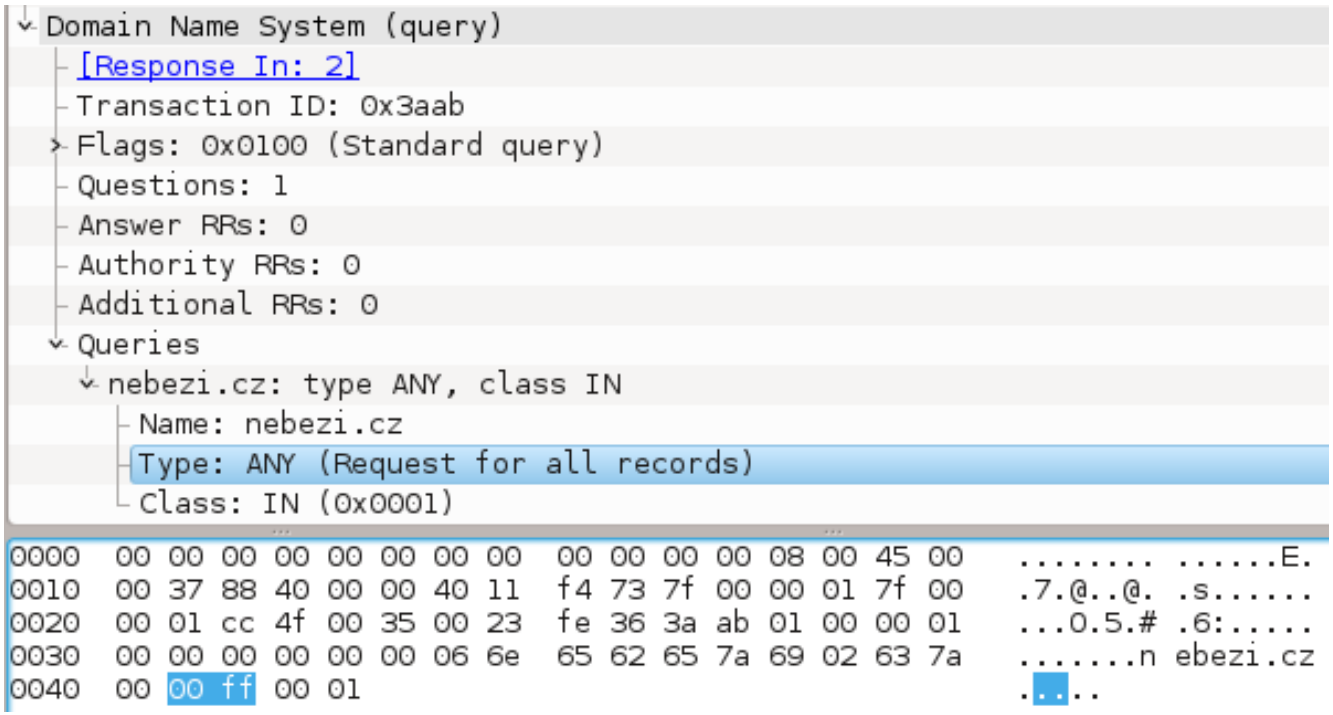
CESNET

Omezení velikosti UDP odpovědi

- rozšíření EDNS0 zvětšuje délku UDP zpráv nad 512 B *obykle na 4096 B*
- omezením velikosti k ~1 kB snížíme úcinnost zesilujícího útoku
- také se tím zlepší situace resolverům s nefunkčním *Path MTU Discovery*
- příliš nízká hodnota může naopak rozbít resolvery bez TCP konektivity
  - obzvláště při použití DNSSEC
  - takto postižených uživatelů je ~2 % (měření Geoffa Hustona)

RRL v linuxovém firewallu

- modul `hashlimit` pro netfilter
- vlastní modul xt_dns pro klasifikaci typu DNS provozu
- více v článku `http://www.root.cz/clanky/zabezpecte-svuj-dns-server/`



Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz