Jak vylepšujeme DNS infrastrukturu pro .CZ?

Zdeněk Brůna • zdenek.bruna@nic.cz • 24. 11. 2017

O čem to dnes bude

- Základní vlastnosti DNS
- Něco o DNS pro .CZ
- Proč posilujeme
- Jak posilujeme
- Co už máme hotovo
- Co ještě připravujeme

Základní vlastnosti DNS

- Domain Name System
- *1983, Hierarchický systém doménových jmen
- Překlad doménových jmen a IP adres
- Režim klient – server
- Stromová struktura

Základní vlastnosti DNS

- DNS servery
  - rekurzivní / **autoritativní**
  - kořenové / **top-level-domain** / nižší
  - primární / **sekundární**

- www.jakfungujedns.cz

- **běží „bez výpadku“**

Něco o DNS pro .CZ

- Autoritativní DNS servery pro .cz
  - [a-d].ns.nic.cz
  - 15 DNS serverů v ČR
  - 16 DNS serverů v zahraničí (DE, AT, UK, SE, 2 x US, CL, JP)
  - vysoká diverzita
    - Debian, Ubuntu LTS, OpenBSD
    - Bind, Knot DNS, NSD
    - Bird, Quagga, BGPD
    - Dell, HP, Intel Cisco, Juniper

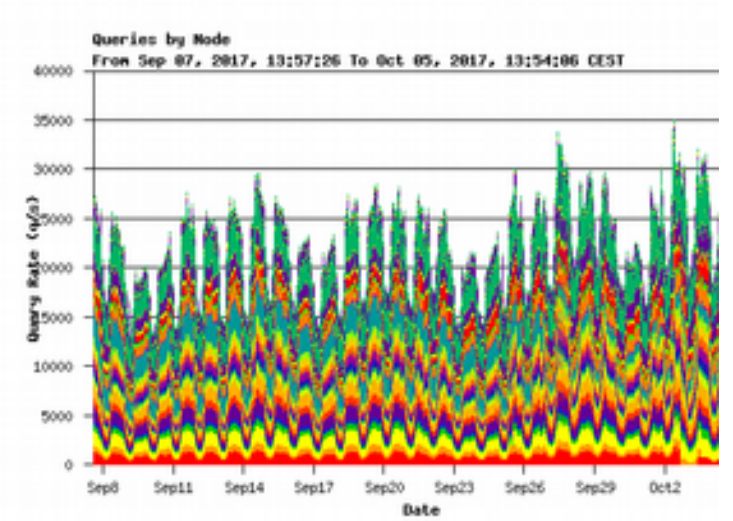
Něco o DNS pro .CZ

- DNS anycast
  - více serverů pod jednou adresou
  - BGP směřuje požadavky do nejbližší lokality
  - rozkládá zátěž, snižuje odezvy
  - přesměrování provozu při výpadku je automatické
  - vhodné umístění DNS serverů

Něco o DNS pro .CZ

Něco o DNS pro .CZ

- Běžný provoz
  - ~ 25 000 Qps
  - ~ 1 miliarda požadavků / den
  - Přibližně 38% DNS provozu z ČR
  - Významné lokality v zahraničí
    - UK (20%), Rakousko (12%), Německo (10%)



Proč posilujeme

- současné limity .CZ DNS anycastu
  - ~ 20 000 000 Qps
  - ~ 60 Gbps
- četnost a síla DDoS roste
  - stovky Gbps, jednotky Tbps
  - distribuovanost (IOT)
- fatální důsledky

Jak posilujeme

- zvýšení odolnosti DNS infrastruktury
  - ~ 200 Gbps / 100 mil. Qps
- ještě větší distribuovanost
  - DNS u ISP / další zahraniční lokality
- zlepšení monitoringu / alertingu
  - zamezení reflection útoků
- zachování diverzity

Jak posilujeme

- upgrade routerů a DNS serverů v ČR (2 lokality)
- navýšení konektivity do NIX.CZ (2 x 100 Gbps)
- zprovozněním několika DNS uzlů u významných ISP
- upgrade významných uzlů DNS anycastu v zahraničí

Jak posilujeme

- DNS stack
  - 1 x router
  - n x DNS server
  - n x switch pro management
  - 1 x server pro management
  - konektivita
    - 1 x IX
    - 1 x tranzit
    - 1 x management

Jak posilujeme

parametr	typ DNS stacku				
	velký	střední	malý	mini	ISP
HW router	ano	ano	ne	ne	ne
IX konektivita	1 x 100 Gbps	4 x 10 Gbps	1 x 10 Gbps	2 x 1/10 Gbps	1 x 10 Gbps
IP tranzit	1 x 10 Gbps	1 x 10 Gbps	1 x 10 Gbps	ne	ne
manag. konektivita	1 x 1 Gbps	1 x 1 Gbps	1 x 1 Gbps	ne	1 x 1 Gbps
počet DNS serverů	30	12	3	2	3
management switch	2 x 48-port	1 x 48-port	ne	ne	ne
management server	1	1	1	0	1

Jak posilujeme

- Proč 30 serverů na velký stack?
  - výkonnost routeru ~ množství DNS serverů ~ konektivita
    - nejmenší pakety 84 B: 100 Gbps / 672 bps ~ 148 809 523 pps
    - běžná velikost DNS odpovědí 512 B: 100 Gbps / 4 096 bps ~ 24 414 062 pps
    - největší pakety 1 538 B: 100 Gbps / 12 304 bps ~ 8 127 438 pps
    - uvažujeme 1 mil. response/s na jeden DNS server (https://www.knot-dns.cz/benchmark/)
    - při „průměrné“ velikosti odpovědi 512 B využije jeden DNS server cca 4 Gbps
    - → pro 100 Gbps konektivitu postačuje 30 serverů
    - při maximální velikosti odpovědi 1 500 B využije jeden DNS server cca 12 Gbps
    - → předpokládá se připojení DNS serverů pomocí 10 Gbps uplinku do routeru

Jak posilujeme

- DNS stack u ISP
  - instance autoritativního DNS serveru s .cz zónou u ISP
  - inspirace u SIDN.NL
  - propagace jednoho z anycast prefixů do sítě ISP
  - využití jen v síti ISP (není povolena propagace do upstreamů/peerů)

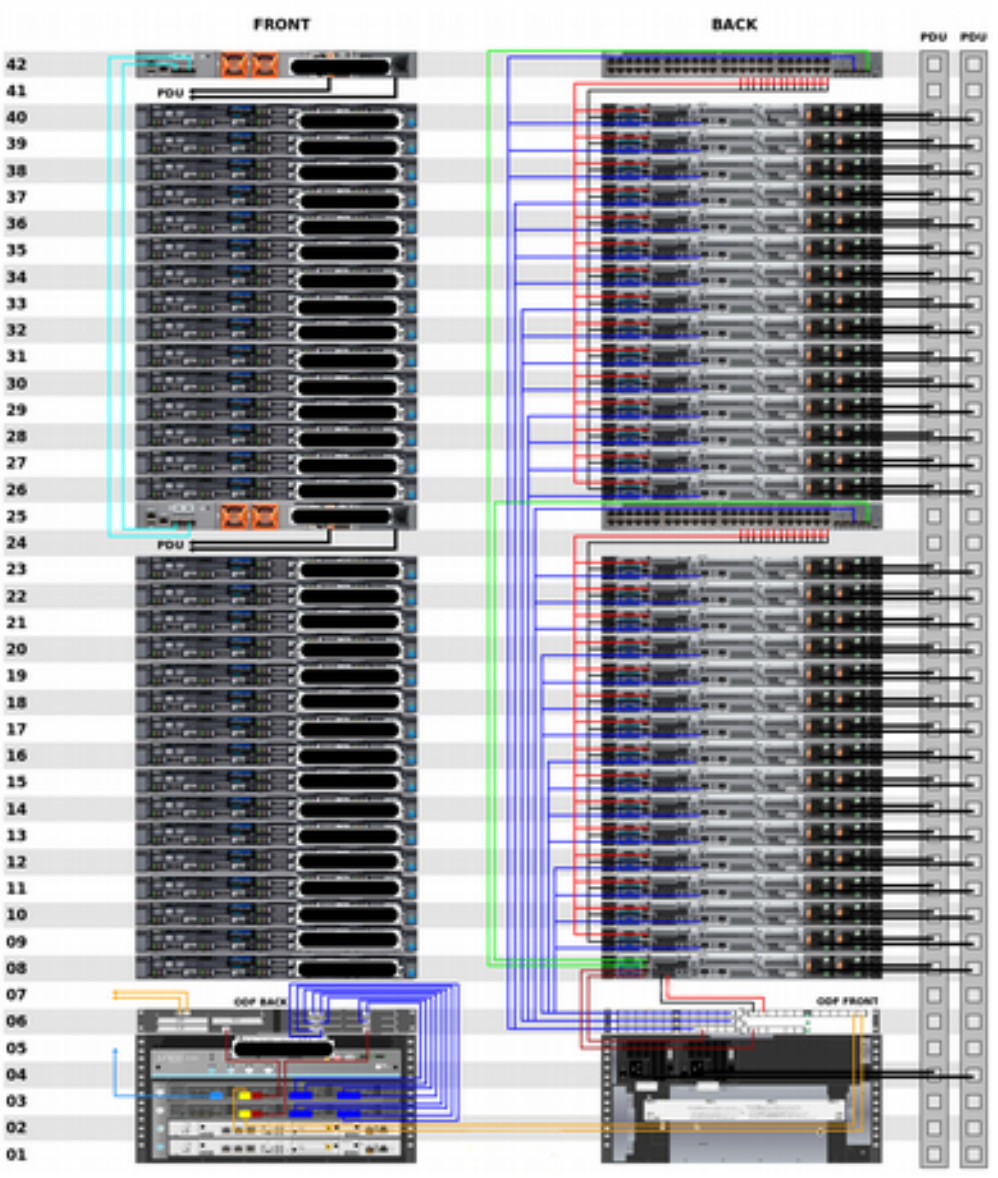
    \+ dostupnost služby DNS v případě útoků proti veřejným DNS serverům

    \+ útok vedený v síti ISP je ukončen „uvnitř“

Co už máme hotovo

- **Upgrade DNS v ČR – první velký DNS stack**
  - lokalita DC TOWER
  - vysokozátěžový rack (10 kW)
  - router Juniper MX240
  - 30 DNS serverů DELL PE R430
  - management server
  - upgrade na 100G do NIX.CZ
  - dokončujeme …

Co už máme hotovo



Co už máme hotovo

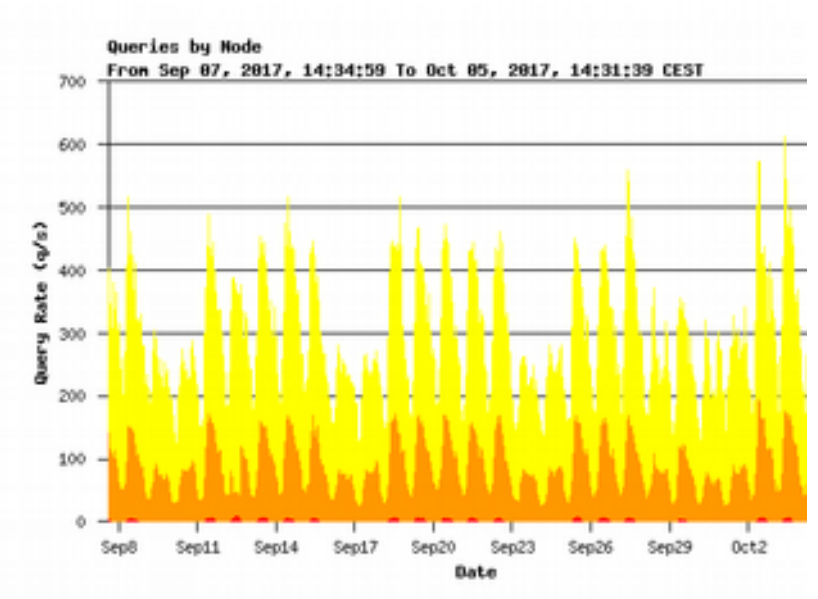
Co už máme hotovo

Co už máme hotovo

Co už máme hotovo

Co už máme hotovo

- 2 x ISP DNS stack



Co už máme hotovo

- **posílení DNS v UK - malý DNS stack**
  - Londýn - LINX
  - 3 DNS servery v jedné lokalitě
  - 1 x management server
  - 1 x Linuxový router s BIRDem
  - upgrade na 10G
  - dokončení v 12/2017

Co ještě připravujeme

- **Upgrade DNS v ČR – druhý velký DNS stack**
  - lokalita DC CECOLO
  - vysokozátěžový rack (10 kW)
  - router ???
  - 30 DNS serverů HP Proliant DL360 Gen9
  - management server
  - upgrade na 100G do NIX.CZ
  - Q1 2018

Co ještě připravujeme

- **posílení DNS v dalších zemích - malý DNS stack**
  - primárně DE, AT
  - nové stacky jinde – analýza (CA, JV Asie)
- **vylepšení monitoringu**
  - zamezení reflection útoků
  - pokusíme se řešit interně – ADAM
- **upgrade vybraných datových propojů na 100 Gbps**

Co ještě připravujeme

- **instalace dalších ISP DNS stacků**
  - alespoň 3 významné ISP
- **DNS stack pro FENIX**

Co ještě připravujeme

- **posílení týmu systémových správců**
- **specialista na analýzu DNS provozu**
  - https://www.nic.cz/page/321/kariera-v-cznic/

Děkuji za pozornost

Zdeněk Brůna • zdenek.bruna@nic.cz