Upgrade DNS anycastu

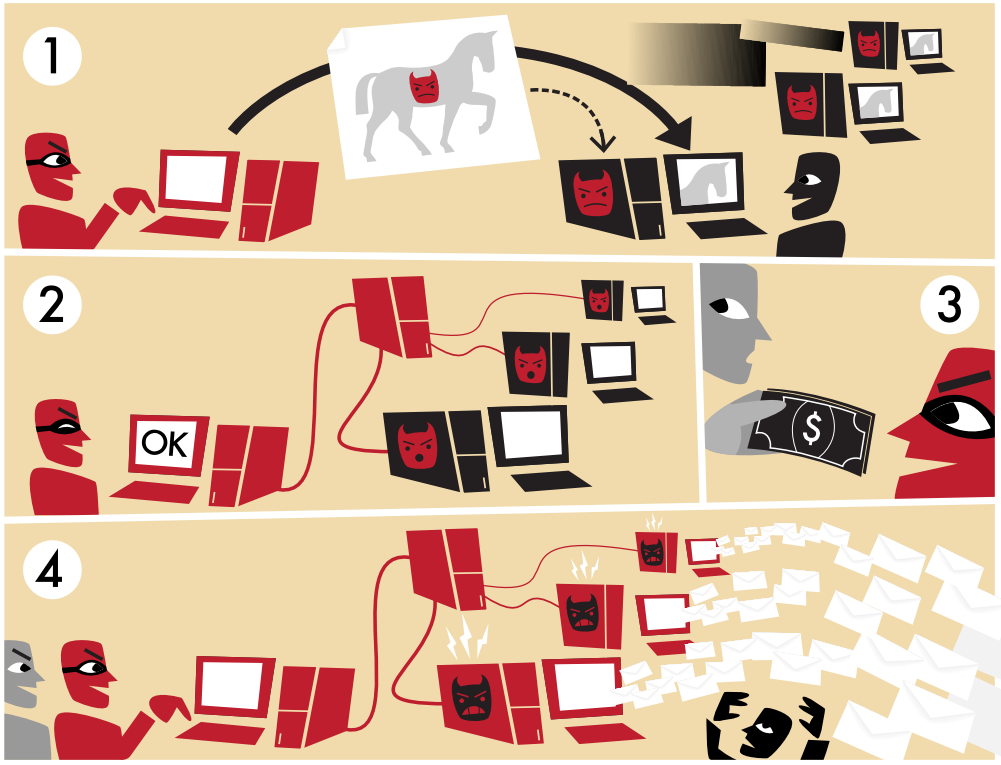
Druhý 100 Gbps stack

Václav Steiner • vaclav.stseiner@nic.cz • 15. 11. 2018

CZ.NIC | SPRÁVCE DOMÉNY CZ

Upgrade DNS anycastu

DDoS na Tureckou doménu



DDoS na Tureckou doménu - předtím

- NIC.TR
- V 2015 6 NS v 5 různých lokalitách
  - 4 NS u ISP-A a 1 NS u ISP-B, 1 NS v Evropě
- Průměrná data na server
  - Datový tok 1.5 Mbps
  - 1 250 dotazů/sekundu

[2015] DDoS na Tureckou doménu

- Útok probíhal od 14.12. 2015 tři týdny, pak byl přesměrován na finanční a vládní sektor
  - veřejné DNS resolvery a autoritativní DNS servery
- DNS Amplification Attack
  - 25% PC v botnetu bylo z tureckých IP adres
  - UDP flooding, spoofování packetů (src/dest 53), aplikační útoky na TCP
- V 09-17:00, 185 000 QPS na server → 148x více
- Datový tok u jednoho z ISP byl až 220 Gbps

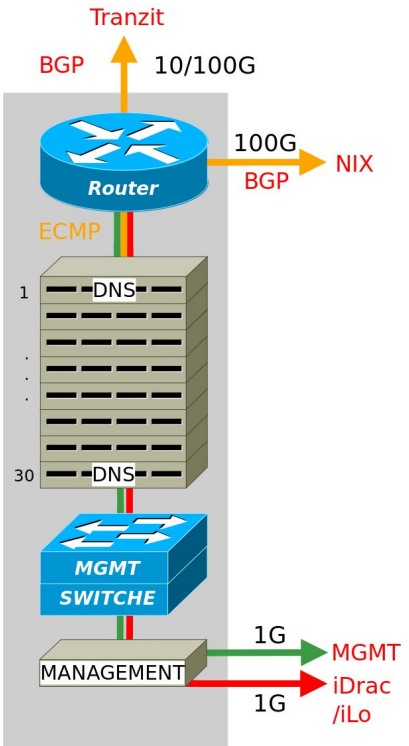
DDoS na Tureckou doménu – poté

- Upgrade infrastruktury v roce 2016
  - 8 NS pro doménu .TR
  - 12 NS pro domény II. Řádu
  - Celkem 100+ serverů

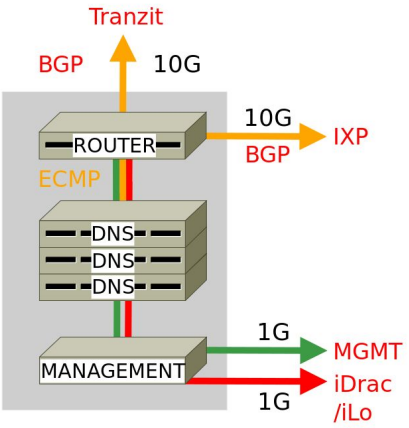
Upgrade DNS anycastu

Koncept DNS stacků

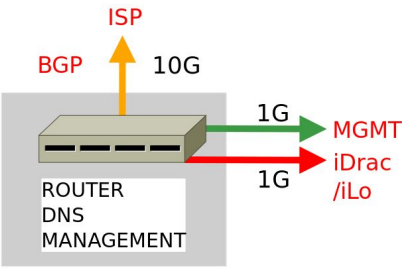
Velký stack



Malý stack



ISP mini



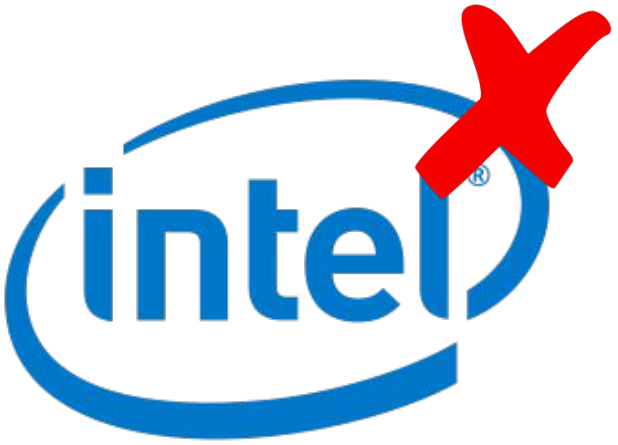
Výběrové řízení – Velké DNS stacky

- Důraz na diverzitu HW
- První a druhý 100 Gbps stack od jiného dodavatele
- Jedno výběrové řízení
  - Router a management switche
  - Servery
- Náročné hodnocení, mnoho kritérií, nejvyšší důraz na splnění technických parametrů

Výběrové řízení - servery

První 100 Gbps stack

30x PowerEdge R430
1x PowerEdge R630



Druhý 100 Gbps stack

31x DL360 Gen9 8SFF

Výběrové řízení – síťové prvky

BROCADE

CISCO

Druhý 100 Gbps stack

Router ASR-9904
2x Nexus 3048
2x Nexus 3232C

JUNIPER NETWORKS

Druhý 100 Gbps stack

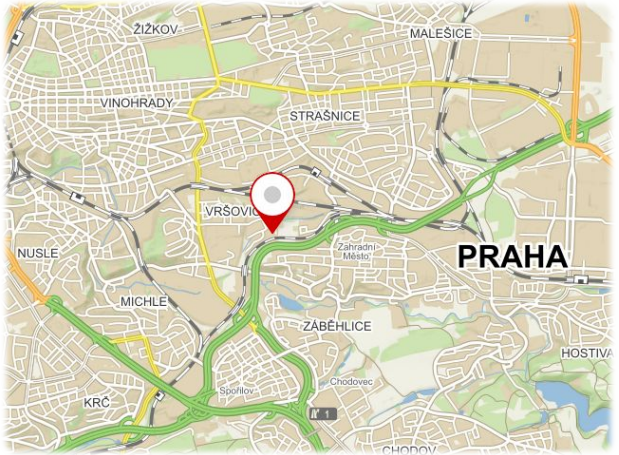
Router MX240
2x EX3400-48T-AFI

NOKIA

HUAWEI

Datacentrum pro druhý 100 Gbps stack

- Druhý 100 Gbps stack je umístěn v datacentru CE Colo (SITEL) na pražském Bohdalci
- V současné CZ.NIC kleci



Rack pro druhý 100 Gbps stack

- Conteg RSF-48-80/120 v barvě RAL 9005
  - Výška 48U, šířka 800mm, hloubka 1 200mm, nosnost 1 500kg
- HDWM-VMR-48-19/10F a HDWM-VMR-48-12/10F
- 2x PDU AP8886
  - napájení 3F, 1x 32A, 400V AC

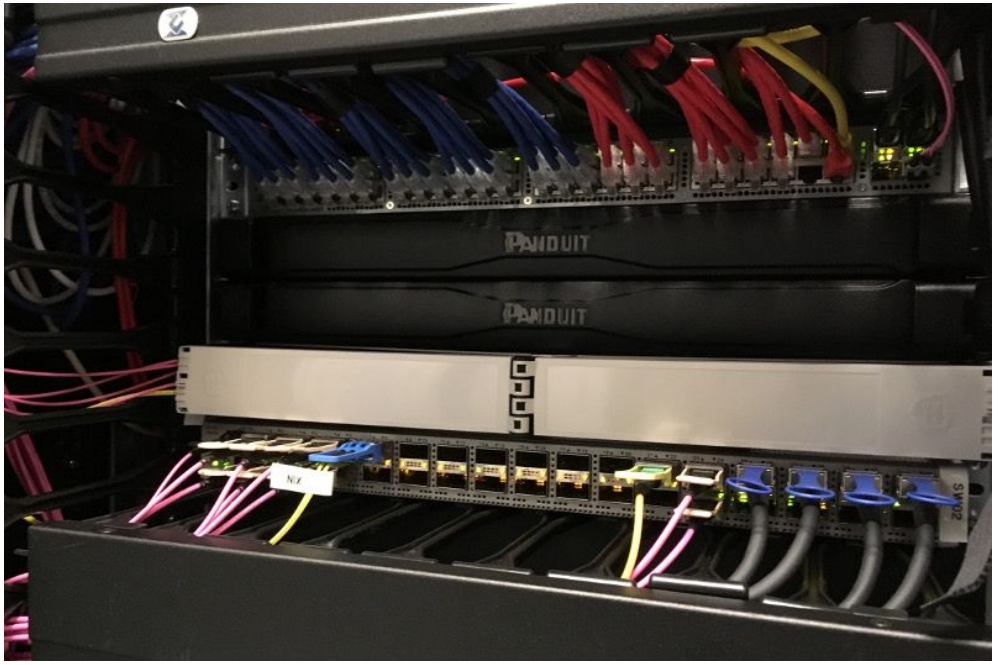
Router pro druhý 100 Gbps stack

- CISCO ASR-9904, 6U

Konfigurace

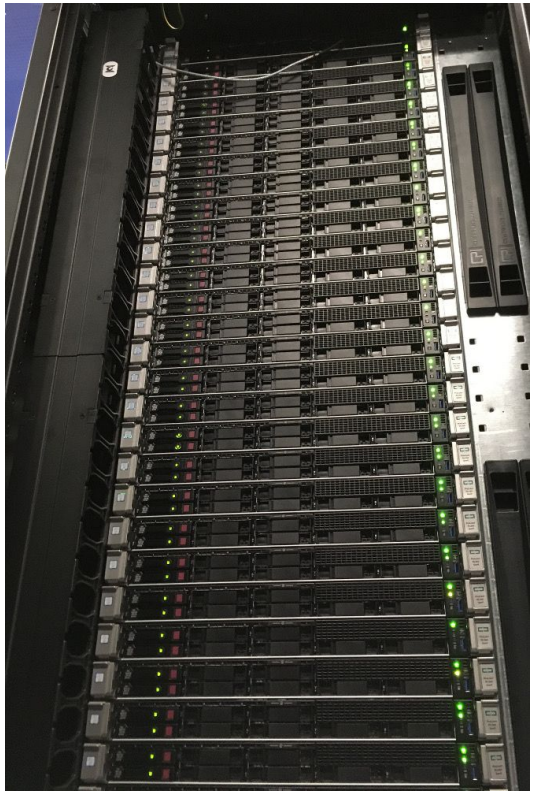
- 2x RSP 880
- 2x 400G modular line karty
- 2+2 MPA moduly 1x 100GE
- CFP2 to CPAK

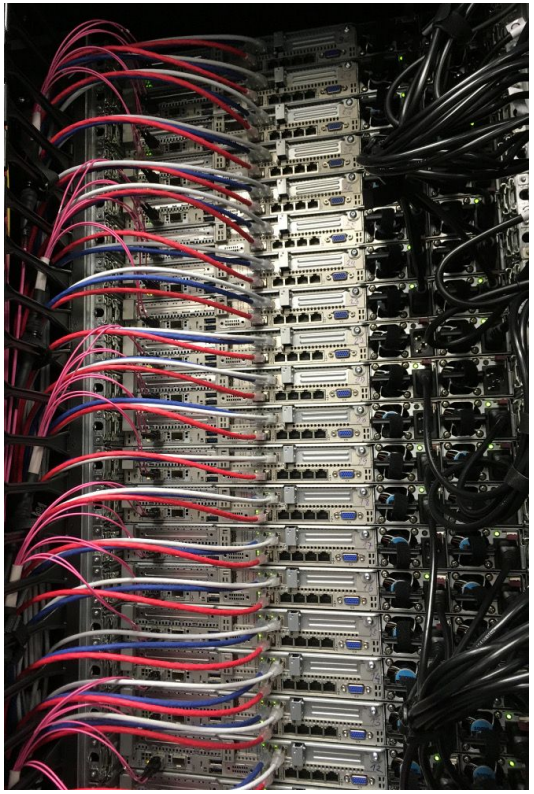
Switche pro druhý 100 Gbps stack



- 2x Nexus 3048 - iLO a správu celého stacku
- 2x Nexus 3232C - Rozplety 40Gb MPO → 4x 10Gb LC pro DNS servery
- 4x MPO/MPO MM OM4 s routerem
- IANOS EDR pro projení se stávající infrastrukturou

Servery pro druhý 100 Gbps stack





- HPE DL360 Gen9 8SFF

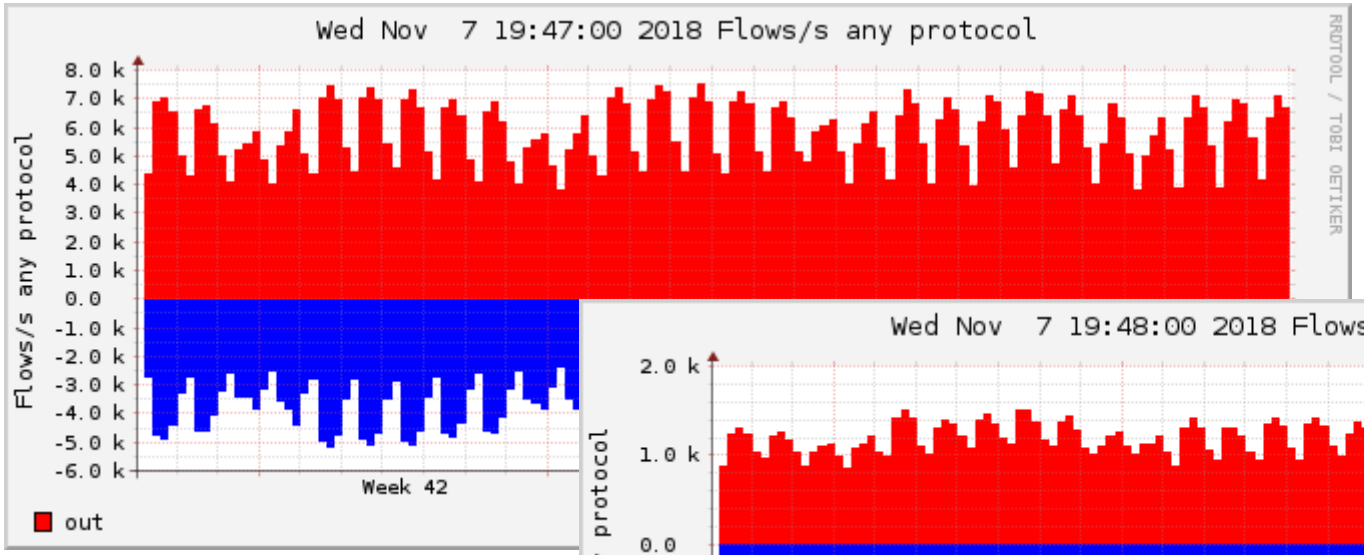
  DNS servery
- 1x E5 2650v4, 32GB RAM
- 2x 300 GB SAS, 1x 2p 10Gb Eth.

  MGMT server
- 2x E5 2680v4, 64GB RAM
- 7x 1,2TB SAS, 4x 2p 10Gb Eth.

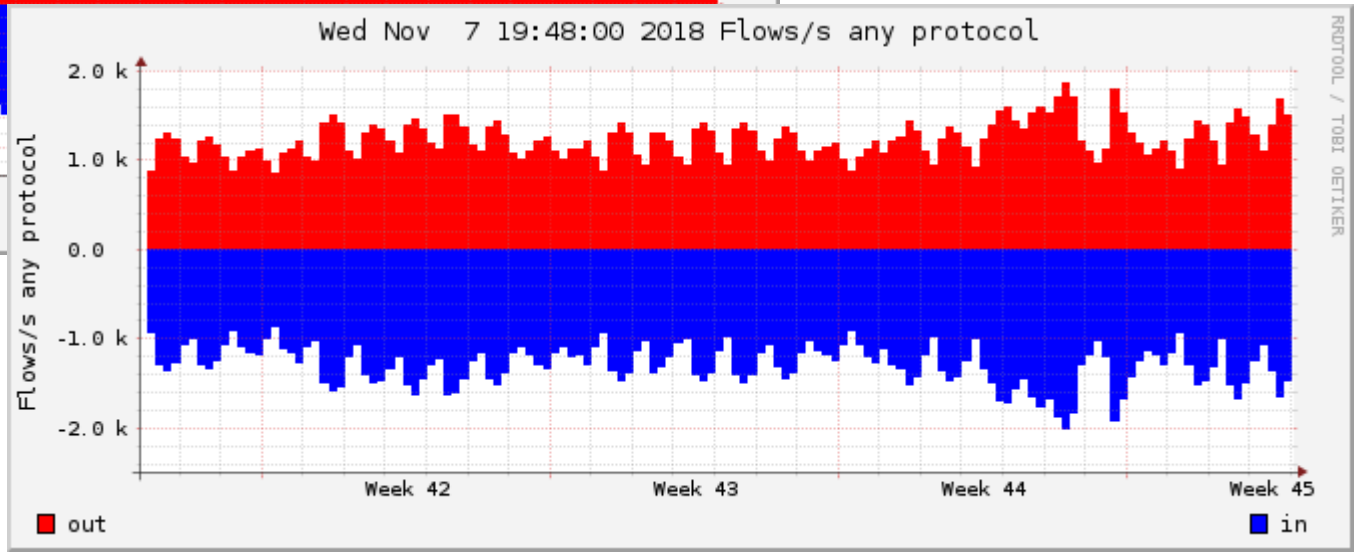
Konektivita pro druhý 100 Gbps stack

- 1x 100 Gbps do peeringového uzlu NIX.CZ
  - Celkem první a druhý velký stack: 200 Gbps do NIX.CZ
- Od 1.11. 2018 proveden upgrade z 10 → 100 Gbps do tranzitu
  - Celkem první a druhý velký stack: 120 Gbps do tranzitu

Doména .CZ – počet DNS dotazů

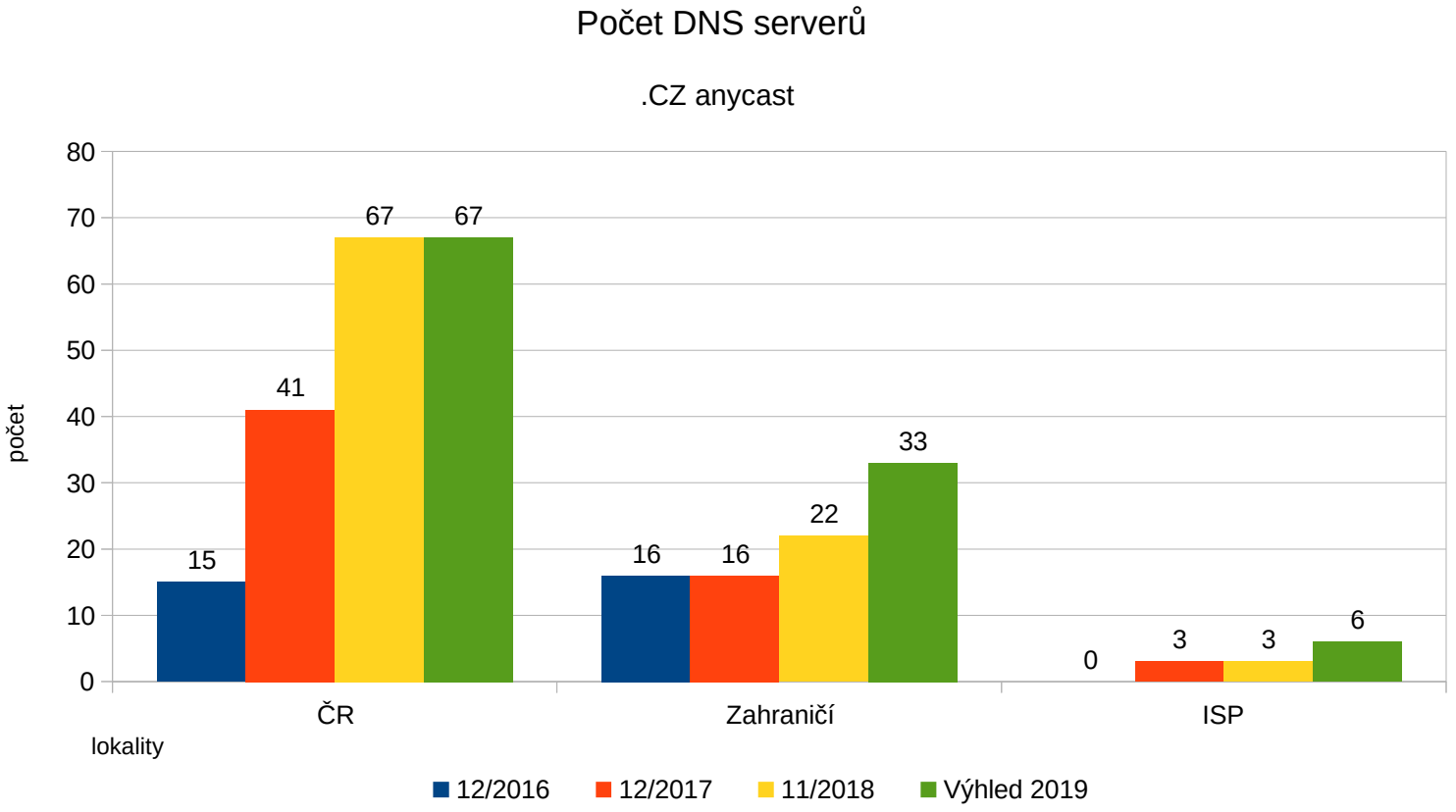


První 100 Gbps stack

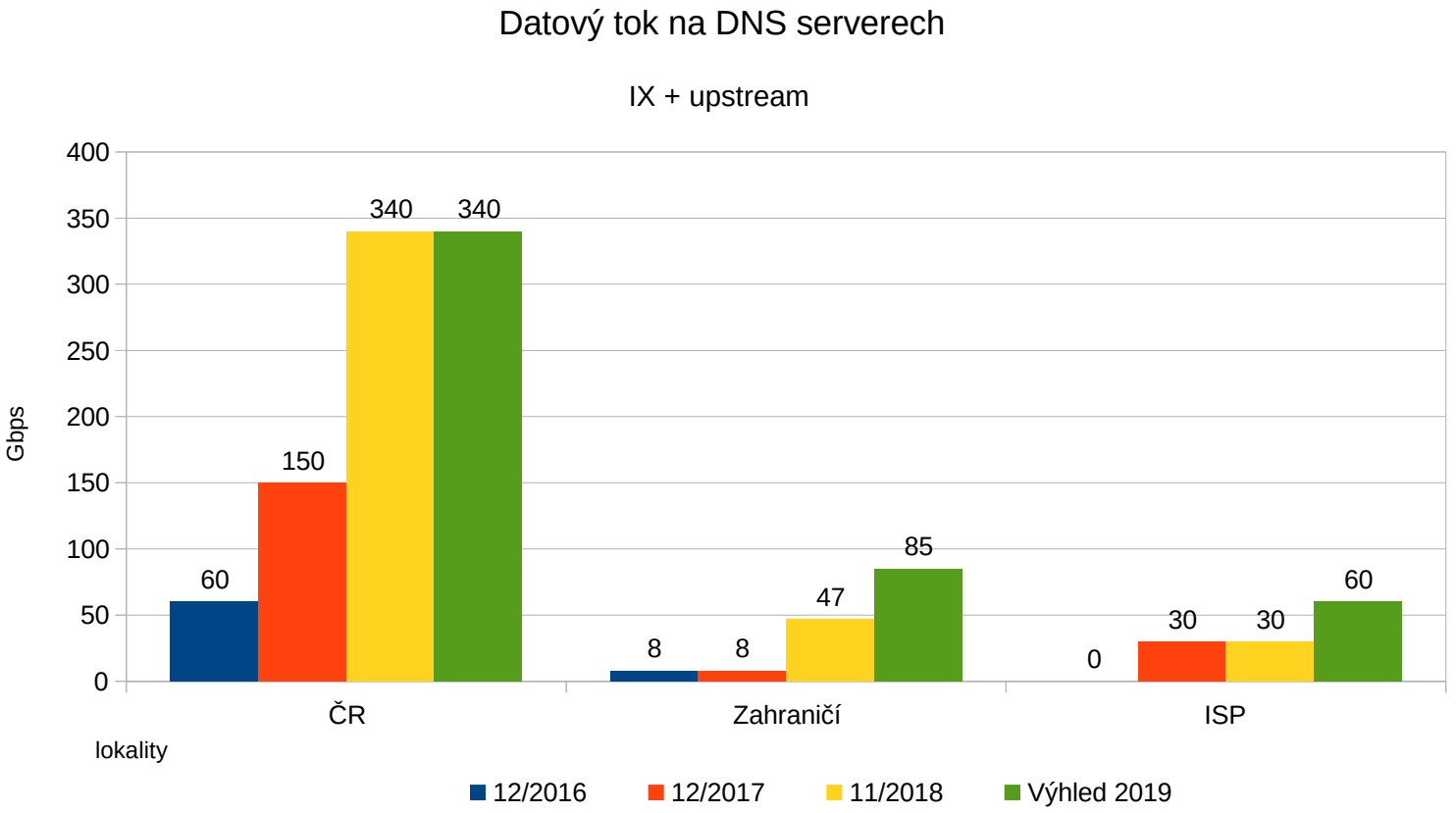


Druhý 100 Gbps stack

Upgrade DNS Anycastu



Upgrade DNS Anycastu



Upgrade DNS Anycastu

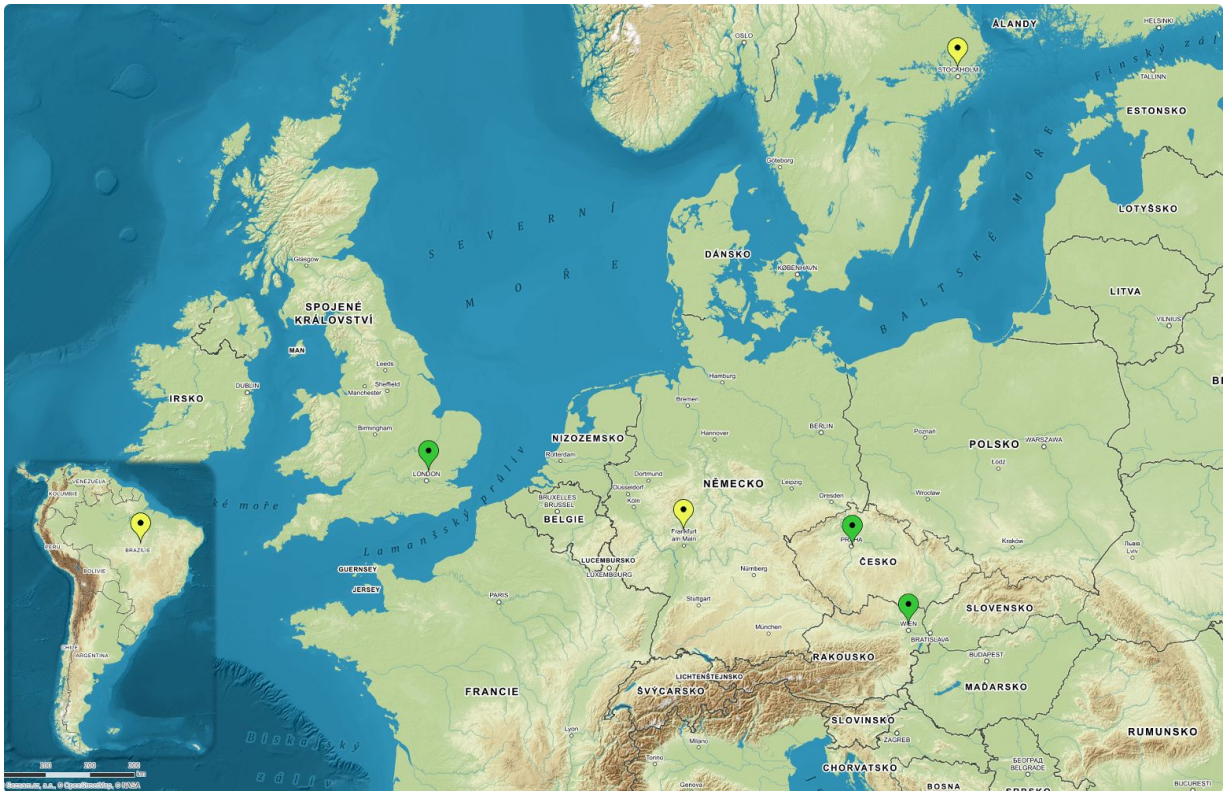
Velký DNS stack v ČR

- 12/2017 – První 100 Gbps
- 10/2018 – Druhý 100 Gbps

Malý DNS stack

- 01/2018 – Velká Británie
- 04/2018 – Rakousko
- v roce 2019 nás čeká:

  Německo, Švédsko, Brazílie



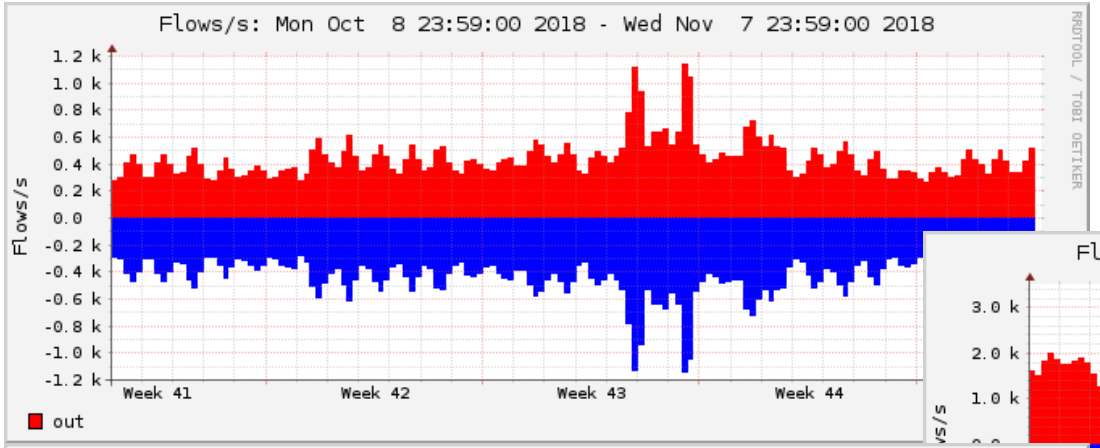
To ještě není konec ...

Doména .CA

- Obdobně již hostujeme domény Makedonie, Tanzánie a Angoly

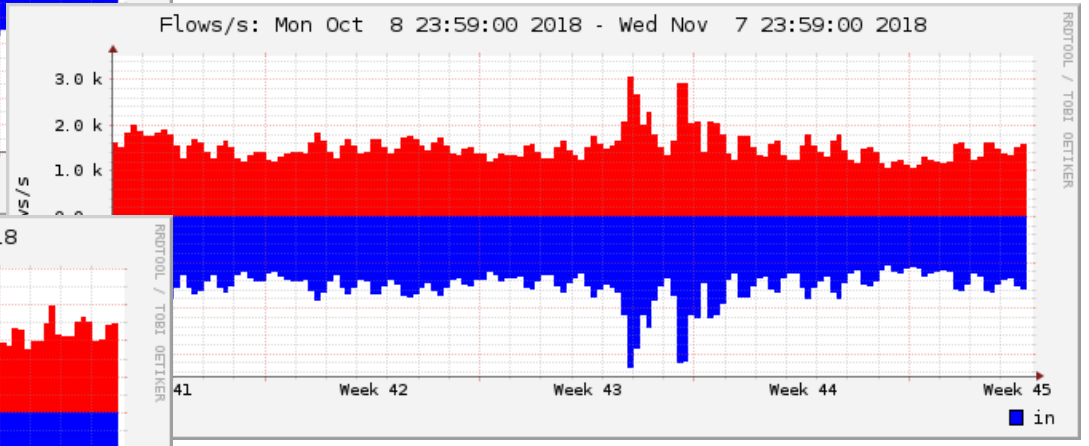
- CIRA (https://cira.ca)
- Hostování .CA ve vybraných lokalitách
  - ČR, Rakousko, Velká Británie
- ~ 2.7 milionu domén
- Sdílení kapacity DNS serverů; mnohonásobně vyšší, než je reálné využití

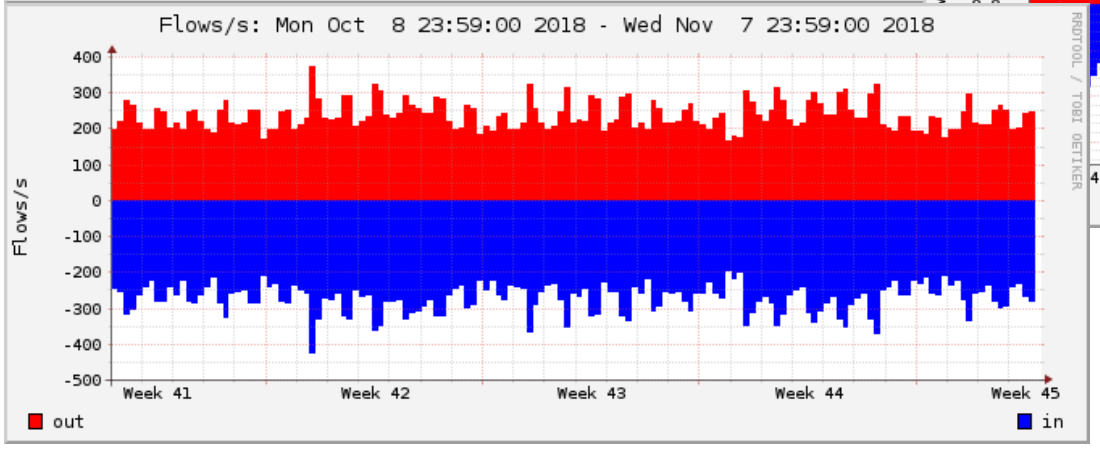
Doména .CA – počet DNS dotazů



ČR

Velká Británie





Rakousko

Ukázka z provozu...

- Hledání doménových jmen metodou Brute force

Source	Destination	Length	Info
193.29.206.1	193.86.108.180	804	Standard query response 0x9075 No such name A oujyfk.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	804	Standard query response 0x2d8c No such name A oujyfg.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	799	Standard query response 0xed6b No such name A oujyfs.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.86.108.180	193.29.206.1	94	Standard query 0x2fca A oujyhc.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0xc28b A oujyht.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x47e8 A oujyha.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x4254 A oujyhd.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0xa950 A oujyhe.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x755d A oujygk.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x7760 A oujygj.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x3ed3 A oujygn.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x080b A oujygx.cz OPT
193.29.206.1	193.86.108.180	799	Standard query response 0xa950 No such name A oujyhe.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	799	Standard query response 0x4254 No such name A oujyhd.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	804	Standard query response 0x2fca No such name A oujyhc.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	799	Standard query response 0x47e8 No such name A oujyha.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	804	Standard query response 0x755d No such name A oujygk.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	804	Standard query response 0x7760 No such name A oujygj.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	799	Standard query response 0xc28b No such name A oujyht.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	804	Standard query response 0x080b No such name A oujygx.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.29.206.1	193.86.108.180	799	Standard query response 0x3ed3 No such name A oujygn.cz SOA a.ns.nic.cz NSEC3 NSEC3 NSEC3 RRSIG RRSIG RRSIG RRSIG OPT
193.86.108.180	193.29.206.1	94	Standard query 0xf1d2 A oujygi.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x4367 A oujygg.cz OPT
193.86.108.180	193.29.206.1	94	Standard query 0x560a A oujygu.cz OPT

Děkuji za pozornost

Václav Steiner • vaclav.steiner@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

Zdroje

- Krists Luhaers – https://unsplash.com/photos/AtPWnYNDJnM
- Google Street View – https://maps.google.com
- Seznam mapy – https://www.mapy.cz
- Conteg – https://www.conteg.cz
- Dr. Attila ÖZGİT - .tr DDoS Attack
- Wikipedia