CZ.NIC | SPRÁVCE DOMÉNY CZ

ISP DNS stack

1 Účel a výhody

ISP DNS stack je označení pro instanci/e autoritativního DNS serveru obsahující CZ ccTLD zónu v interní síti cizího subjektu (dále jen „ISP“). Tato služba je primárně určena velkým ISP, kteří poskytují internetové služby většímu množství zákazníků a jsou tedy z pohledu CZ.NIC významným uživatelem DNS provozu.

Tato DNS instance propaguje anycast prefix právě jednoho z CZ.NIC DNS anycastů do sítě ISP. CZ.NIC si vyhrazuje právo definovat, který ze současných běžících DNS anycastů bude využit. Současně má také právo tento zvolený DNS anycast v průběhu času změnit za jiný. ISP však nemá povolen tento prefix propagovat dále do svých upstreamů nebo svým peerům.

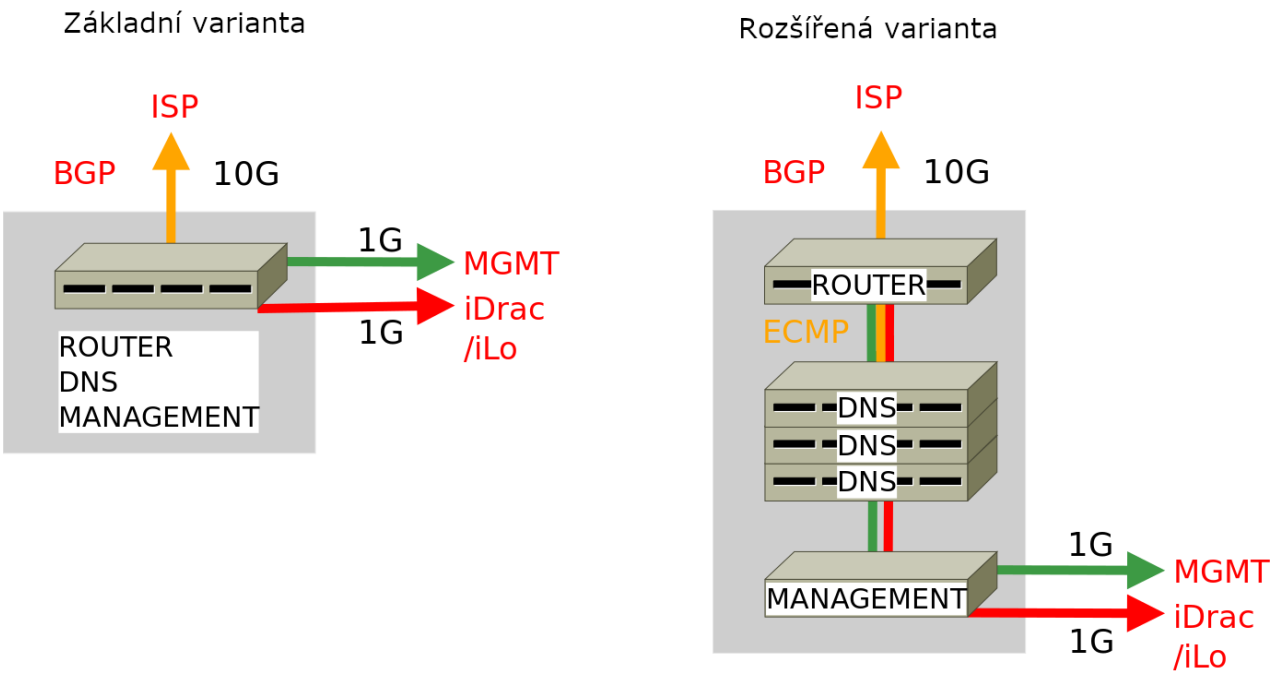
Hlavní výhodou provozu takové DNS instance z pohledu ISP je plná dostupnost služby DNS v případě útoku proti veřejným autoritativním DNS serverům CZ.NIC. Zákazník v síti ISP tak není útokem ovlivněn a služba DNS je pro něj plně dostupná. Vzhledem k principu anycastu dále umístění ISP DNS stacku v síti ISP snižuje latenci a zrychlení odezev DNS dotazů zákazníkům v síti ISP.

Naopak výhodou pro CZ.NIC je, že pokud je útok na službu DNS veden z interní sítě ISP, bude ukončen pouze na této DNS instanci. Útok se tak dále nešíří, tj. nedochází k ovlivnění veřejných autoritativních DNS serverů. Současně může ISP na tuto událost reagovat, útok řešit a nezávadný DNS provoz přesměrovat na veřejné autoritativní DNS servery.

2 Architektura

Pro většinu ISP je dostatečným řešením jeden nezávislý DNS server, viz obr. níže, který je schopen obsloužit přibližně 100 milionů DNS požadavků za den. Jedná se o tzv. *Základní variantu ISP DNS stacku*.

V případě vyššího objemu DNS požadavků lze řešení rozšířit, konkrétně například na řešení z pěti serverů v tzv. *Rozšířená varianta ISP DNS stacku* s oddělenými službami (3x DNS server, 1x management a monitoring server, 1x router), který dokáže obsloužit trojnásobek DNS provozu.



3 Provoz

ISP DNS stack je ve výhradní správě CZ.NIC ve smyslu provozu operačního systému a všech na něm běžících služeb. ISP provider zajišťuje nákup potřebného hardware a jeho provoz ve vlastní síti, umístění v datacentru, konektivitu do internetu spolu s potřebnými IP rozsahy a BGP session.

Základní varianta ISP DNS stacku spravuje CZ.NIC za 5 000,- měsíčně. Pro Rozšířenou variantu platí cena 20 000,- měsíčně.

Pro členy FENIXe platí 50% sleva.

4 Požadavky na HW a konektivitu

Pro Základní variantu ISP DNS stack postačuje 1 server Dell PowerEdge nebo HPE ProLiant. Protože server(y) spravuje CZ.NIC (instalace, monitoring atp.) je nutné trvat pouze na vyzkoušených vendorech a konfiguracích HW.

- CPU: rok výroby 2018+, minimálně 8 jader
- RAM: minimálně 32GB
- HDD: minimálně 2x 300GB (SATA/SAS/SSD)
    - RAID1 ideálně se spare diskem
- NETWORK (viz požadavky na konektivitu dále):

- 1x 1/10G připojení pro dns provoz (preferujeme Intel karty X710)
- 1x 1/10G připojení pro management (oob)

- BMC (viz požadavky na konektivitu dále):
  - 1x 1/10G připojení pro dedikovaný management port serveru (iLO, iDrac)
  - KVM konsole, virtualní media, podpora HTML5

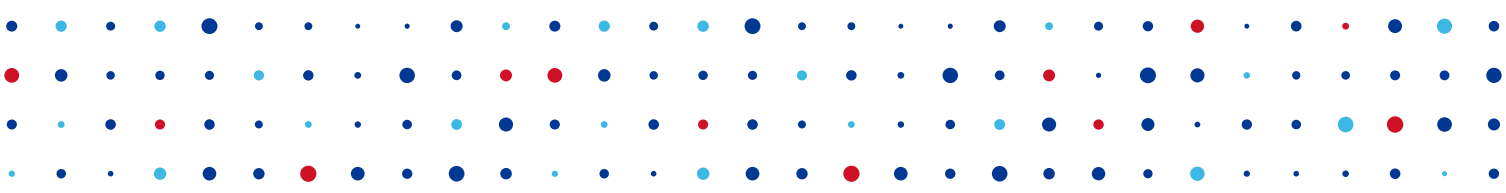
Hardwarovou konfiguraci pro Rozšířenou variantu ISP DNS stacku dodá CZ.NIC na vyžádání.

Síťová konektivita & BGP

1) 1x 10G připojení pro dns provoz
   - rozhraní pro privátní BGP peering - propagace anycast prefixu viz BGP peering dále
   - dual stack (IPv4 + IPv6) adresace
   - (pro ISP, z pohledu dns serveru):
     - příchozí provoz:
       - `bgp` - TCP/179 (peering adresy)
       - `dns` - TCP/53, UDP/53 (na propagovaný cz anycast prefix)
       - `bfd` - UDP/3784 (peering adresy)
     - odchozí provoz:
       - `bgp` - TCP/179 (peering adresy)
       - `dns` - TCP/53, UDP/53 (z propagovaného cz anycast prefixu)
       - `bfd` - UDP/3784 (peering adresy)

2) 1x 1/10G připojení pro management (oob)
   - rozhraní pro management serveru (instalace, monitoring, aktualizace zóny atp.)
   - dual stack (IPv4 + IPv6) adresace
   - (pro ISP, z pohledu dns serveru):
     - neomezený příchozí provoz (přístup z Internetu). Předpokládaný provoz:
       - `icmp`
       - `ssh` - TCP/22
       - `dns` - TCP/53, UDP/53
       - `snmp` - UDP/161
     - neomezený odchozí provoz (přístup do Internetu). Předpokládaný provoz:
       - `icmp`
       - `http(s)` - TCP/80, TCP/443
       - `dns` - TCP/53, TCP/53
       - `ssh` - TCP/22
       - `ntp` - UDP/123
       - `whois` - TCP/43
       - s velkou pravděpodobností nebude server využívat žádné služby daného ISP, takže ISP může „odfiltrovat“ DNS ISP server od „svých“ sítí/služeb

3) 1x 1/10G připojení pro dedikovaný management port serveru (iLO, iDrac)
   - IPv4, IPv6 nebo dual stack (IPv4 + IPv6) adresace
   - (pro ISP, z pohledu dns serveru, **vhodné nastavit na straně ISP - BMC management nemusí mít možnost filtrování**):
     - neomezený přístup ze sítě `217.31.207.144/28` a `2001:1488:800:90::/64`



4) BGP peering:

- CZ.NIC AS: `200070`
- propagace anycast prefixu:
  - `c.ns.nic.cz`
    - IPv4: `194.0.14.0/24`
    - IPv6: `2001:678:11::/48`

5 SLA

CZ.NIC garantuje řešení problémů s provozem serveru a poskytování DNS služby v tzv. NBD režimu. Služba je postavena jako vhodný doplněk pro ISP, nefunkčnost serveru znamená automatické používání veřejných autoritativních serverů.

Podrobnější podmínky provozu služby a technické kontakty jsou uvedeny v dokumentu „Smlouva o spolupráci při provozování uzlu DNS anycast“.

6 Závěr

CZ.NIC si vyhrazuje právo tuto službu nabídnout a provozovat pouze u vybraných ISP, jejichž zákazníci jsou významným uživatelem DNS provozu. Výběr vhodného/ých ISP je prováděn na základě průběžného sběru dat z DNS provozu a tedy tam, kde zvýšení dostupnosti služby a současně odolnosti proti útokům znamená znatelný přínos pro obě strany.