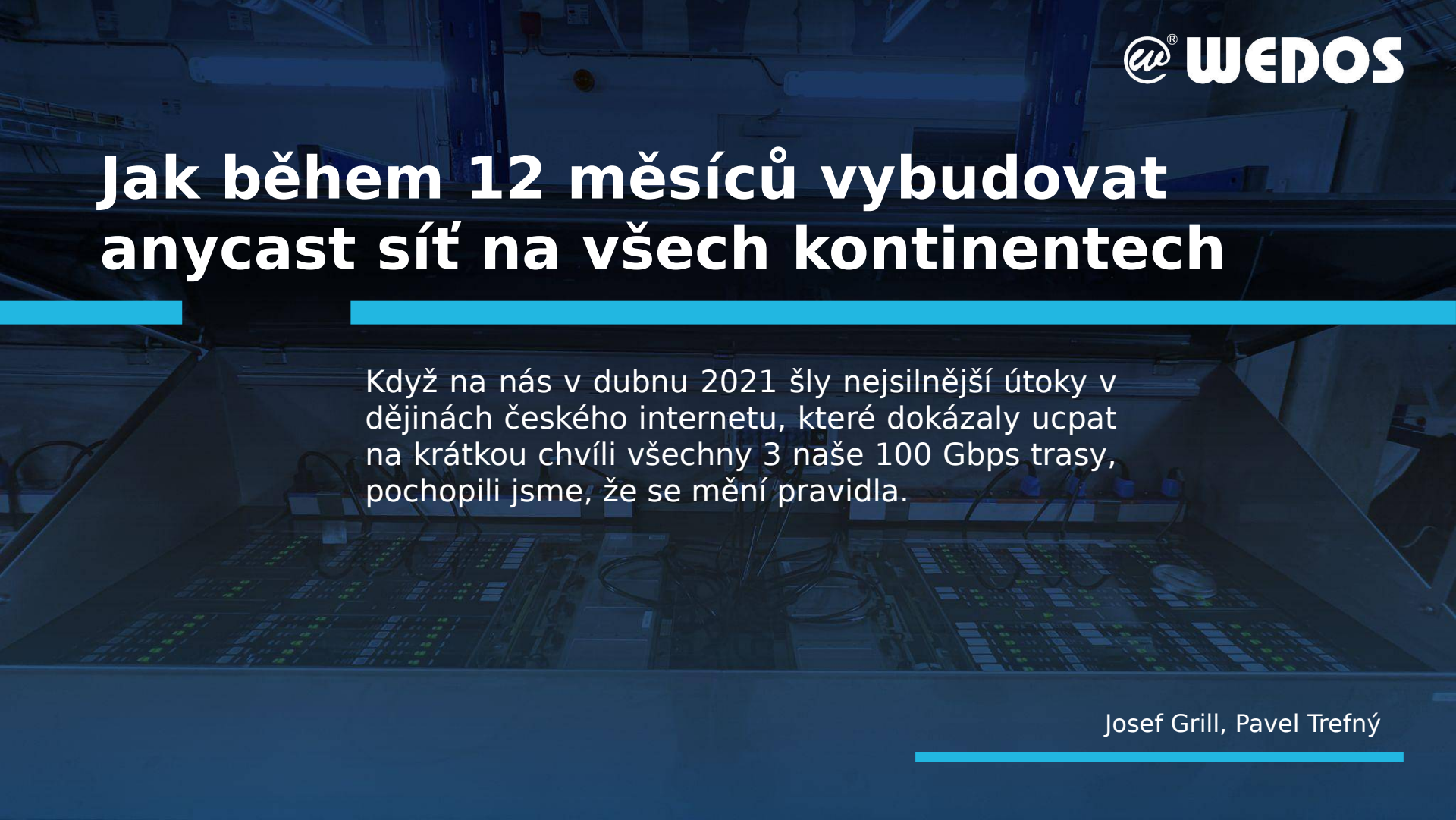

WEDOS



Jak během 12 měsíců vybudovat anycast síť na všech kontinentech

Když na nás v dubnu 2021 šly nejsilnější útoky v dějinách českého internetu, které dokázaly ucpat na krátkou chvíli všechny 3 naše 100 Gbps trasy, pochopili jsme, že se mění pravidla.

Josef Grill, Pavel Trefný

První impuls

- **Doposud jsme se s něčím podobným nesetkali. Jednak tento útok byl mimořádně silný (stovky Gbps) a dlouhý (v podstatě 72 hodin). Chvíli nám trvalo, než jsme se nové aktuální situaci přizpůsobili.**
- **Útočníci zaútočili nejprve na naše routery. Když jsme s tím úspěšně bojovali, tak začali útočit na naše firemní weby. Když jsme i s tímto bojovali, tak začali útočit na zákaznické služby (webhostingy a některé virtuální servery).**
- **Mimochodem nejsilnější naměřený útok na 1 naší službu – jeden náš web byl přes 160 Gbps. Útoky byly samozřejmě různě kumulované a spojované.**
- Špičkově to bylo ucpaných 300 Gbps a přes 200 milionů paketů za sekundu.
- Překvapilo nás jak dokázali pěkně útok sesynchronizovat. Na to že šlo o 2289 IP adres, tak začal doslova během 1 – 2 vteřin.

Bojujeme

- **Postupně jsme všechny 3 trasy vylepšili na 100 Gbps**
- **Trasa 1 – 100 Gbps – DC1 WEDOS ⟶ Tábor ⟶ Praha SITEL (CeColo)**
- **Trasa 2 – 100 Gbps – DC1 WEDOS ⟶ Písek ⟶ Praha SITEL (CeColo)**
- **Trasa 3 – 100 Gbps – DC1 – DC2 WEDOS ⟶ Jihlava ⟶ ČDT (U2) ⟶ TTC**
- **A pak další dvě 10 Gbps záložní trasy**
- **Chytrý switch Arista 7280QR-C36, který používáme jako hraniční “router”, zvládne až 4,32 Tb přenesených dat za vteřinu a nebo 1,44 miliard paketů za vteřinu**

jeden z bodů v oleji

Expadujeme

- **Původně jsme měli v plánu v první fázi rozmístit HPE Moonshoty 1500 do 5 lokací**
- Jeden HPE Moonshot připojen až 320 Gbps konektivitou
- **První bod v zahraničí - Vídeň (Telia - 80Gbps)**
- Množství konektivity - původní předpoklady:
  - 40 Gbps do Telia,
  - 40 Gbps od někoho dalšího (většinou Cogent),
  - 20 Gbps do místního peeringu,
  - 20 Gbps na vlastní propoj mezi našimi body,
  - 40 Gbps rezerva (většinou další peering nebo přímý propoj k někomu).

První lokality

Helsinky

Stockholm

Varšava

Amsterdam

Curych

Paříž

Madrid

Madrid

Budujeme

- **Každá lokalita je samostatně fungující as208414, které je připojeno k několika upsteamům (Cogent, Arelion, CDN77) a lokálním IXP (B-IX,BIX.BG,Equinix).**
- Jednotlivé lokality spolu nejsou vzájemně propojené. Jako router využíváme 2x L3 switch HPE Moonshot-45XGc, který je součástí HPE Moonshot 1500 Chassis.
- Switch máme osazený 8x QSFP nebo 4x QSFP a 16x SFP+ pro uplink. Každý ze 45 serverů má 40 Gbps uplink a je připojený ke každému ze switchů samostatnou 10G linkou.
- Tento switch je v lokalitách kde je víc IXP nedostatečný, protože má limit na 16k IPv4 a 8k IPv6 prefixů.

foto zapojení v Barceloně

Budujeme

- **Místo něj nasazujeme Aristu DCS-7280TR-48C6-R, která je osazena šesti QSFP28 a čtyřiceti osmy metalickými 10G porty.**
- Díky technologii **FlexRoute** se do tohoto boxu vejde zhruba **1.5M IPv4 prefixu.**
- V lokalitách kde používáme jako router **Moonshot-45XGc** zvažujeme možnost nasazení filtrace prefixů na základě doručeného provozu.
- **Ve všech lokalitách domlouváme minimálně 80 Gbps linku, ale ve většině to bude 120-160 Gbps.**

starší ARISTA 7050QX-32S

Shrnutí

- **WEDOS Global využívá technologii BGP anycast**
- Tradiční DDoS ochrana (na 3. a 4. síťové vrstvě), tedy zablokujeme útočníka ještě před tím, než dorazí fyzicky na servery v datacentru
- Ochrana webů (7. síťová vrstva)
- **Celá infrastruktura WEDOS Global má aktuálně k dispozici přes 1500 fyzických serverů a konektivitu přes 2,5 Tbps**
- Do budoucna plánujeme služby jako CDN, VPN atd…
- V březnu bylo zaznamenáno celkem 1,9 miliardy požadavků z 8,7 milionů unikátních IP adres, **dále bylo zablokováno 10,8 milionů požadavků pomocí WAF**
- Infrastruktura WEDOS Global odbavila nejvíce požadavků z Česka (1 259 milionů), USA (190

modul QSFP-LR4-40G

Prostor na Vaše otázky...

Děkuji za pozornost a někdy na shledanou na Hluboké nebo u nás v administraci...

e-mail: hosting@wedos.com
linkedin: WEDOS