DDoS prevention in .cz

Tech Day – ICANN 66

Ondřej Filip • ondrej.filip@nic.cz • 4 Nov 2019 • Montreal
Trigger

- DDoS attack against domain .tr
  - Presented at Tech Day ICANN 60
  - “One ISP reported 220 Gbps attack bandwidth”
- Evaluated on our side - current anycast setup not sufficient
- Some HW tools evaluated – not preventing all attacks
- Result: **Anycast capacity upgrade – focus on Czechia**
Our anycast - World
Our anycast - Europe
Our anycast - Czechia/Prague
Basics for .CZ DNS anycast

- Asia
  - [JP] Tokyo
- Europe
  - [AT] Vienna
  - [CZ] 5 x Prague, 1 x Undisclosed location
  - [DE] 2 x Frankfurt
  - [SE] Stockholm
  - [UK] London
  - [IT] Milan
- North America
  - [US] 1 x California, 1 x Virginia
- South America
  - [BR] Sao Paulo
  - [CL] Santiago de Chile

17 locations
10 countries
4 continents
Upgrade results – number of servers

Czechia
- 01.01.2017: 15
- 11.06.2018: 41
- 30.06.2019: 68

Abroad
- 01.01.2017: 16
- 11.06.2018: 22
- 30.06.2019: 36

ISP
- 01.01.2017: 0
- 11.06.2018: 3
- 30.06.2019: 3
Upgrade results – network bandwidth

Czechia

<table>
<thead>
<tr>
<th>Date</th>
<th>Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>01.01.2017</td>
<td>60</td>
</tr>
<tr>
<td>11.06.2018</td>
<td>150</td>
</tr>
<tr>
<td>30.06.2019</td>
<td>340</td>
</tr>
</tbody>
</table>

Abroad

<table>
<thead>
<tr>
<th>Date</th>
<th>Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>01.01.2017</td>
<td>0</td>
</tr>
<tr>
<td>11.06.2018</td>
<td>8</td>
</tr>
<tr>
<td>30.06.2019</td>
<td>26</td>
</tr>
</tbody>
</table>

ISP

<table>
<thead>
<tr>
<th>Date</th>
<th>Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>01.01.2017</td>
<td>0</td>
</tr>
<tr>
<td>11.06.2018</td>
<td>0</td>
</tr>
<tr>
<td>30.06.2019</td>
<td>30</td>
</tr>
</tbody>
</table>

01.01.2017
11.06.2018
30.06.2019
Upgrade results

- performance limits

- 31 servers → 107 servers
- 20 000 000 → 200 000 000 QPS
- 60 Gbps → 400+ Gbps
Not just performance - diversity

- HW vendors – Cisco, Juniper, Dell, HPE
- SW
  - OS (Ubuntu / Debian / OpenBSD)
  - BGP (BIRD / OpenBGPd / Quagga)
  - DNS (KNOT / BIND / NSD)
- Locations
  - Geographical
  - Different networks (IXP, ISP)
Upgrade results

1st 100 Gbps DNS stack
Upgrade results

2nd 100 Gbps DNS stack
Sharing of the DNS infrastructure
Improving our anycast clouds

- Who sends queries to our servers?
- How long does it take for a query to reach our server?
  - typically active measurement (PING – DNS server vs client or probe)
  - we used ADAM (Advanced DNS Analysis and Monitoring) and passive analysis
    - captured DNS traffic from .CZ DNS anycast (1.-14.5.2019)
    - ~15,65 billion+ queries
      - UDP: 99.87% ~ 15,63 billion queries
      - TCP: 0.13% ~ 21 million queries
Improving our anycast clouds

• median RTT of a TCP handshake for each pair (client + server)

• evaluated RTT for each:
  • client
  • network
  • country
  ...

[Diagram of DNS server and client exchanging packets]
Improving our anycast clouds

For each pair (client, server) compute median RTT of a TCP handshake

<table>
<thead>
<tr>
<th>client_ip</th>
<th>client_cc</th>
<th>client_asn</th>
<th>server</th>
<th>queries</th>
<th>tcp</th>
<th>median_rtt</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] AT, Vienna</td>
<td>37123</td>
<td>0</td>
<td>NA</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Undisclosed</td>
<td>5171434</td>
<td>57</td>
<td>12.7 ms</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha – CE</td>
<td>2579707</td>
<td>6</td>
<td>11.9 ms</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha - CRA</td>
<td>27065563</td>
<td>220</td>
<td>11.5 ms</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] UK, London</td>
<td>8416765</td>
<td>88</td>
<td>43.4 ms</td>
</tr>
</tbody>
</table>
Improving our anycast clouds

Evaluated RTT = weighted mean of RTT for all servers

<table>
<thead>
<tr>
<th>client_ip</th>
<th>client_cc</th>
<th>client_asn</th>
<th>server</th>
<th>queries</th>
<th>median_rtt</th>
<th>weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] AT, Vienna</td>
<td>37123</td>
<td>NA</td>
<td>0.0009</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Undisclosed</td>
<td>5171434</td>
<td>12.7 ms</td>
<td>0.120</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha – CE</td>
<td>2579707</td>
<td>11.9 ms</td>
<td>0.0596</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha - CRA</td>
<td>27065563</td>
<td>11.5 ms</td>
<td>0.625</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] UK, London</td>
<td>8416765</td>
<td>43.4 ms</td>
<td>0.195</td>
</tr>
</tbody>
</table>

\[
RTT = \sum_{i=1}^{n} \text{Norm}(w_i) \cdot RTT_i \quad \text{for } RTT_i \neq NA
\]

Evaluated RTT for 217.31.193.164 = 17.9 ms
Query distribution
RTT by country

Evaluated RTT [ms]
- Less than 10
- 10 to 30
- 30 to 75
- 75 to 150
- 150 to 300
- 300 or more
- No data
Queries vs RTT (Regions)

Number of queries vs evaluated RTT by region
For DNS traffic captured on 1-14 May 2019

- Africa
- Americas
- Asia
- Europe
- Oceania

Continent

- Africa
- Americas
- Asia
- Europe
- Oceania
Queries vs RTT (TOP 50 Countries)

Number of queries vs evaluated RTT for top 50 countries by query number
For DNS traffic captured on 1-14 May 2019
## Traffic distribution (Example)

### DNS traffic distribution vs evaluated RTT for countries in Eastern Europe (with min. 0.01% share in traffic)

For DNS traffic captured on 1-14 May 2019

<table>
<thead>
<tr>
<th>Source of DNS queries</th>
<th>ipv4</th>
<th>ipv6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Czechia (29.44% 8ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Russia (3.15% 44ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slovakia (2.06% 11ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Poland (0.81% 29ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ukraine (0.33% 43ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Romania (0.22% 34ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hungary (0.22% 19ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bulgaria (0.13% 35ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Belarus (0.07% 39ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moldova (0.03% 42ms)</td>
<td></td>
</tr>
</tbody>
</table>

### Queries (UDP+TCP) over server distribution (within each country)

- 10.0%
- 20.0%
- 30.0%
- 40.0%

### Evaluated RTT

- <10 ms
- 10-30 ms
- 30-75 ms
- 75-150 ms
- 150-300 ms
- NA

**Europe Eastern Europe (36.45% 34ms)**
A DNS map from Czechia
Conclusions

- Trying to prevent DDoS by brute force
- Monitoring using our tool set called ADAM
- Still expanding – looking for partners in NA, AP and AF
- And BTW evaluating creating own HW – combination of FPGA and many ARM mini servers
Thank you!

Ondřej Filip • ondrej.filip@nic.cz • https://www.nic.cz