CloudFlare DNS Anycast Services

Ólafur Guðmundsson I olafur@cloudflare.com

Network

- Over 80 locations soon
- All services over Anycast

CloudFlare DNS expertise

- Deliver DNS answers in fast and reliable manner worldwide
- Extensive experience in absorbing large DDoS attacks
  - Multilayer defense architecture
  - We answer less than 1% of DNS packets, and no-one complains
    - As most are attack packets
- Hard to use us as amplifiers
  - We block most attack traffic, and DNS packet size is kept under 512 bytes

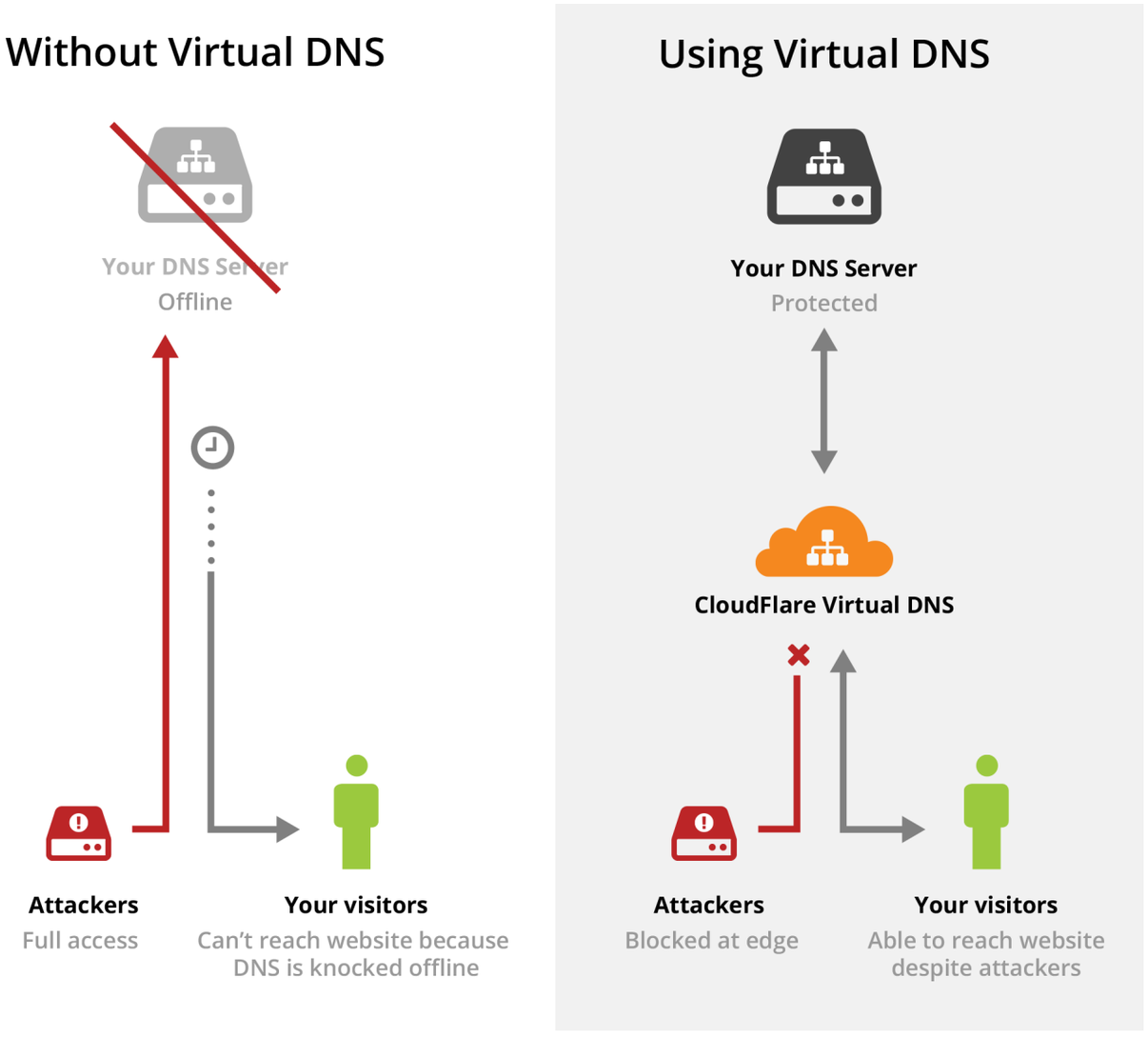
DNS services: RRDNS

- Highly distributed authoritative server
- DNSSEC signing on the fly
- Data entered via API/UI replicated to edges in seconds
- FAST and reliable
- “ANY” suppressed

```
dig cloudflare.com ANY

cloudflare.com.     3788   IN HINFO "Please stop asking for ANY"
 "See draft-ietf—dnsop-refuse-any”
```

DNS products: Virtual DNS



- A proxy authoritative server
- We will cache data requested and answer from edge
- Intelligent fetching of answers from origins.
- No need to update us if zones added/deleted

The cost of staying online?

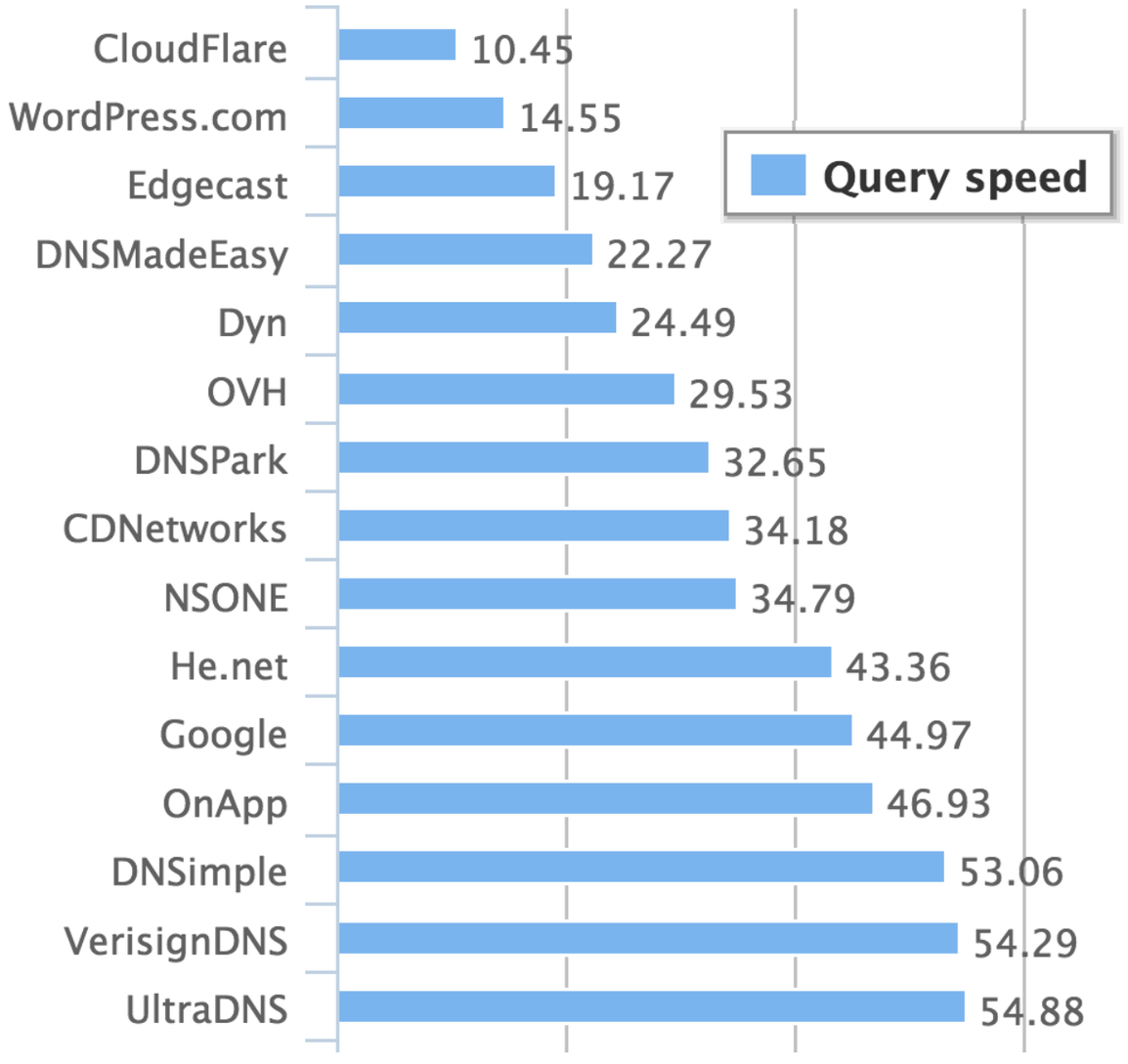
- Providers need to capacity plan for attacks
  - We have mitigated 5xx Mp/s attacks
- Attacks evolve all the time
  - we see them all

19 DNS attack(s) / 44.11M pps

20 SYN attack(s) / 38.29M pps

The new norm of DNS

- Anycast delivery
- Defense in depth
- DNSSEC on the fly
- Smaller answers
  - No need for 5-13 NS records
  - RSA needs to be retired (Key sizes 5x bigger than ECDSA)
  - Suppress ANY



dnsperf.com