

IPv6 at IRCcloud

Stories from the end of thousands of IRC connections

About IRCCloud

- Modern hosted IRC client & bouncer
- Tiny UK-based ex-startup
- Four employees
- Emphasis on reliability and cost

Tech details

- ~20,000 active outbound IRC connections
- ~1500 lines of IRC chat per second (>20,000 peak)
- >10TB stored IRC logs
- ~30 servers, in managed and cloud hosting

IPv6

- IPv6 support for many years
- ~65% of all outbound IRC connections are v6
- Unique IPv6 address per user, aids abuse prevention

2017: script kiddies are still DoSing people on IRC

- Unsophisticated, volumetric DDoS attacks
- Probably from off-the-shelf tools/services
- 2-4 attacks >1Gbps per week
- Largest (known) attack: ~120Gbps, 50kpps (in 2015!)
- Frequency is irregular but seasonal (school holidays)

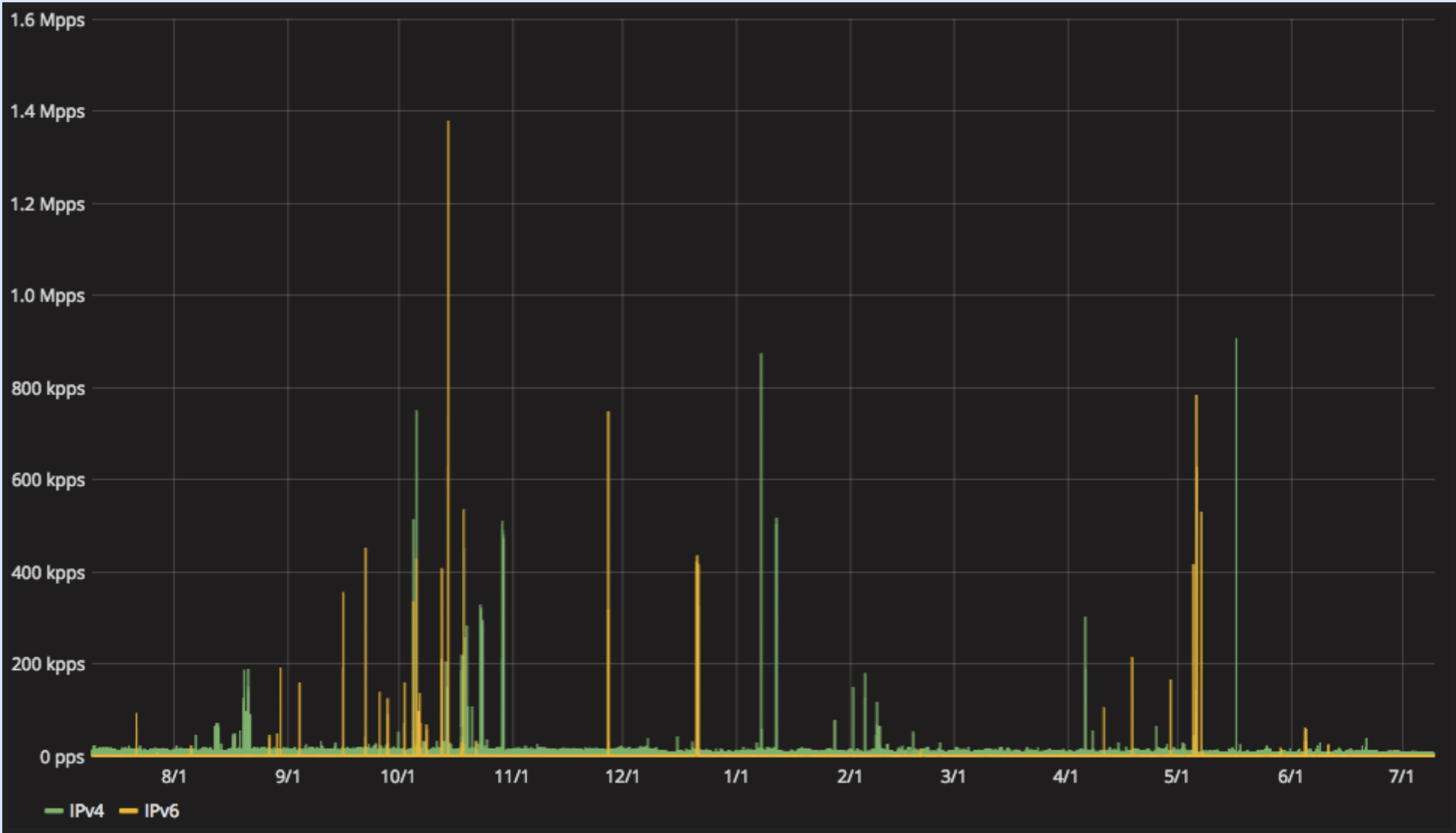
DDoS protection is essential

(no, we can't "just use CloudFlare"!)

- TCP connection uptime is key
- Running our own network would be costly
- DDoS-protected managed hosting seems the only viable option

DDoS-protected managed hosting

- Many of these refuse IRC-related customers (!)
- Many of the cheaper services are bad
- The best services are pricey
- ...and they're still not great



(measured at the edge)

IPv6 DDoS

We first saw a v6 DDoS around 2015. Recent v6 DoSes are now larger than our gigabit edge ports. Still, nobody seems to care yet.

In theory, v6 DoS is easier to mitigate

(for us, at least)

Blackholing the attacked user's v6 IP is preferable to blackholing a v4 address handling many users.

Thank You

Email: russ@irccloud.com

Twitter: [@russss](https://twitter.com/russss)

IRC: [russss on chat.freenode.net](https://chat.freenode.net)