Contribution ID: **95** Type: **not specified**

Multidimensional fair-share rate limiting in BPF

Tuesday, August 25, 2020 9:00 AM (45 minutes)

As UDP does not have flood attack protections such as SYN cookies, we developed a novel fair-share ratelimiter in unprivileged BPF, designed for a UDP reverse proxy, that is capable of applying rate limits to specific traffic streams while minimizing the impact on others. To achieve this, we base our work on Hierarchical Heavy Hitters, which proposes a method to group packets on source and destination IP address, and we are able to substantially simplify the algorithm for our rate-limiting use case in order to allow for an implementation in BPF.
We further extend the concept of a hierarchy from IPs addresses to ports, providing us with precise rate limits based on the 4-tuple.

Our approach is capable of rate limiting floods originating from single addresses, subnets but also reflection attacks, and applies limits as specific as possible. To verify it's performance we evaluated the approach against different simulated scenarios.
The outcome of this project is a single library that can be activated on any UDP socket and provides a flood protection out of the box.

I agree to abide by the anti-harassment policy

I agree

Primary author: OTTEN, Jonas (Cloudflare)

Co-author: BAUER, Lorenz (Cloudflare)

Presenters: OTTEN, Jonas (Cloudflare); BAUER, Lorenz (Cloudflare)

Session Classification: Networking and BPF Summit

Track Classification: Networking & BPF Summit