Towards a Federated Anycast Network

In this presentation, we propose the use of a federated anycast environment running at NRENs as a way to improve DNS resilience against DDoS attacks.

In recent years, we noticed several universities moving infrastructure services to commercial clouds as a way to improve service resilience. More than technical aspects, to host services in commercial cloud implies costs, dependency, and data protection policy. An alternative to this model is to build your anycast network and set up the service in the cloud. However, this requires management, expertise, and proper tools to run and deploy anycast nodes.

NRENs have a long history of cooperation, as seen on Eduroam service. We believe that this cooperation model, based in federations could also be used for anycast services. More than sharing a private cloud, we propose to build a federated anycast service where institutions can host and operate their services.

Domain Name System (DNS) service is the first case that could be in a federated anycast network. Failures on name servers usually are catastrophic, causing major outages on services and websites. Moreover, DNS is a light way service in terms of computational and networks requirements. Making it a service easy-to-host.

On the other hand, DNS servers are also frequently used in amplification attacks. To avoid this misuse DNS Administrators need to be aware of current and new techniques to solve this issue [1]. A recent research located 30-40 thousand distinct name revolvers inside educational networks have the potential to be misused to attack other sites. [2]. Further, countermeasures as DNS response rate limiting to avoid DNS amplification attacks has a low adoption of roughly 10% [3]. Normally, DNS security is not a priority issue to be addressed in all universities.

In the past, universities exchanged DNS zone files to prevent emails from being lost due to a failure in mail exchange (MX) name resolution. Nowadays, we use a technique called anycast to spread these copies. IP anycast uses the same IP address on several geographically distributed sites, relying on the routing system to allocate the best server for a client. Anycast is widely used in the DNS infrastructure, NTP services, content delivery networks, certificate authority, and distributed denial of service (DDoS) mitigation.

Somehow, the biggest research networks and universities already use local anycast instances to load-balance services like DNS and LDAP. However, research networks are region-specific: GEANT covers Europe, RNP covers Brazil, Internet2 covers the US, and a dozen of others around the world. This regionally limits the potential of anycast, making it difficult to deflect DDoS against a specific domain. Just worldwide networks can fully explore the potential of anycast to improve performance and resiliency against DDoS.

In this context, a federated anycast network can achieve a global anycast infrastructure. However, on the creation of any federated services, the biggest challenge is centered on political and laws issues. NRENs already had succeeded in federated services, and the technical feasibility is the first step.

In this presentation, we analyse the requirements needed to build such infrastructure focusing on safety, resilience, privacy, and domain isolation. We also provide an overview of opportunities, risks, and challenges needed to build such infrastructure. This includes operational matters (e.g., pertaining to the correct and reliable operation), administrative matters (e.g., pertaining anycast addressing and hosting use), and routing matters (e.g., pertaining to Internet transit use). We design an environment looking a those main requirements while developing a set of tools able to optimize anycast use, and improve the performance and resilience against DDoS.

References

[1] A. Rizvi, "Anycast agility: Adaptive routing to manage DDoS," 2022.

[2] R. Yazdani, "Mirrors in the Sky: On the Potential of Clouds in Reflection and Amplification DDoS," 2022.

[3] C. Douglas, "The best bang for the byte: Characterizing the potential of dns amplification attacks."