{* SECURITY *}

Why global DDoS protection is essential for Anycast networks

‘If you don’t have Anycast it’s not a good DNS service’

John E Dunn Tue 18 Jan 2022 // 11:55 UTC

PAID FEATURE In October 2021, in an incident lasting more than six hours, Facebook *disappeared* from the Internet. This wasn’t a temporary .com outage on the company’s primary domain but a complete shutdown of its public existence that also dragged into the darkness WhatsApp, Instagram, and Messenger.

What had happened? The popular assumption was a DDoS attack, but experienced heads knew this highly unlikely for a company well defended from such attacks. What about the company’s Domain Name Servers (DNS)? That seemed more likely, but it was still hard to comprehend that an entire global DNS network could fail at once.

In fact, DNS was involved, albeit because of a configuration screw-up originating with the glue that makes routing traffic between these name servers possible, Border Gateway Protocol (BGP). So, not DNS itself but still a timely reminder of how important DNS has become. The Facebook outage was a perfect illustration of the most significant property of DNS – nobody notices it until it’s not there and everything has gone to pot.

The last 20 years has seen growing worry about the vulnerability of these services to a range of forces including the provisioning complexity that caught out Facebook. Security has also loomed large with the warning shots being two infamous DDoS attacks on the Internet’s root DNS servers in 2002 and 2007, the first of which saw global DNS performance slump alarmingly on the 13-server core servers. The system stayed up – just – but the alarm was palpable. Five years later, attackers tried a repeat with curious results – despite the attack being 10 times the size and duration, only two of the 13 servers struggled in the same way.

It turned out those two were the only DNS root servers still using traditional IPv4 unicast DNS as opposed to a newer and more robust technology called IP Anycast. Traditionally, DNS services were provisioned using unicast, an addressing scheme in which every DNS server is assigned a single IP address.

Dating back to the 1980s, this is hugely inefficient; if a server becomes overloaded with traffic, the only option is to try a backup server from a list at the expense of increased latency. Anycast, by contrast, allows numerous name servers to be hidden behind the same IP address with traffic routed to the topologically nearest one to maximise performance and efficiency.

Anycast boom

Anycast's advantages were understood in principle, but it took the DDoS attack in 2007 to shift the dial for DNS Anycast as big Content Delivery Networks (CDNs), and top-level domain (TLD) registrars adopted the technology at speed. The next job was to sell DNS Anycast to everyone else, which resulted in big companies such as Google, Cloudflare, and Verisign entering the market.

Interestingly, big tech hasn't monopolised the market. As with the rise of broadband ISP services in the early 2000s, DNS Anycast has seen smaller specialist companies thrive too. One of these is RcodeZero DNS (the name references the DNS term for a *no error*), launched in 2011 to provide DNS Anycast services by sister company ipcom GmbH, itself a spin out of nic.at, the domain registry for the Austrian national .at TLD.

A key player in the company's emergence was Klaus Darilion, who started as a VoIP engineer at nict.at but has served as RcodeZero DNS's Head of Operations since its founding. At first, business was slow. Then, around five years ago, the idea that Anycast was a mainstream technology took hold and business started to grow. Today, RcodeZero DNS provides Anycast DNS to numerous TLDs, including Ireland, the EU, Finland, Hungary, The Netherlands, Belgium, Portugal, Poland, and Slovenia. It also boasts a growing number of commercial customers and service providers.

"We didn't have the intention to make big money out of it. We wanted to build a rock-stable service for ourselves while getting some compensation for these costs by providing an Anycast service to top level domains," says Darilion.

“After the first year we had one customer. It takes some time to get a reliable name in this community and at first people are conservative and don’t adopt every new technology. Now everybody has found out that if you want to have lots of name servers around the world and a stable service, Anycast is the only option.” Today, Dariilon tells us, “more than 20 international TLDs with almost 21 million domains and more than 100 providers and companies with about 3.8 million domains trust in RcodeZero DNS”.

The company’s network, configured as two separate clouds, now numbers between 40 and 50 servers in 20 sites across the world, a mixture of servers configured by RcodeZero itself backed by commercial cloud servers. “This supports three products: two high-end services aimed at TLD registries and ISPs, and a mainstream service for enterprises.”

“Enterprises often only protect one or two domains, but they still want rock-solid service for their very important domains on a 24x7 basis,” says Darilion.

What makes one Anycast provider different from any other and why use a smaller provider at all? Darilion’s answer parallels why some businesses prefer to use smaller, specialist ISPs over larger rivals – customer service.

“If you use Google and you have a problem when you call up you can wait days or weeks for an answer. It’s more or less impossible to get in touch with an engineer. We’re a small company and these requests go rapidly from level to level. With us, you end up talking to an engineer who is dealing with the service.”

This includes a 24x7 emergency hotline. Similarly, if a customer has a feature request. “A few times we have implemented a feature simply because the customer requested it. For example, the DNSSEC signing service, which is included free of charge in every RcodeZero DNS bundle, will become increasingly important. This is a complex, specific topic that we have addressed extremely effectively. Many registrars are looking to outsource this service.’

Coping with BGP

Despite its clear advantages, Anycast comes with a steep learning curve, which RcodeZero DNS had to grapple with in its early days. Most of this has to do with the fact that Anycast (unlike unicast, multicast and broadcast) was

originally developed in the 1990s for IPv6 and is implemented for IPv4 through BGP network routing. In this environment, the room for mistakes is non-existent.

“For Anycast to work, you have to know how Internet global routing and BGP works. But we were DNS guys, not network guys. We had to learn it the hard way over several years. Even now, 50 per cent of the work at RcodeZero DNS is maintaining perfect global routing,” agrees Darilion.

The DNS side is no easier. Forget popular descriptions of the Internet as a fibre optic marvel; it is first and foremost a giant routing system with a lot of leeway for providers in how they distribute traffic. This can have major implications for anything connected to DNS which is incredibly fussy about latency.

“It doesn’t make sense to put an Anycast server in the US and end up with a lot of traffic from Asia on it. We end up doing a lot of background checks on the backbones of service providers to make sure it is a good idea to put one of our servers there.”

An independent company like RcodeZero DNS must first work out where and with whom it can host Anycast infrastructure. “If you’re Google, getting Anycast to work is simple because you have data centres everywhere.”

DDoS is out there

So much for performance and latency, but the much darker topic of DDoS attacks is never far away in any discussion of DNS resilience. While Anycast reduces the impact of DDoS attacks in principle, it’s not always that simple.

“Even using Anycast, you’ll still get DDoS attacks. Of course, the more servers you have, the more you can handle attack traffic from small DDoS attacks. The problem is there are also big DDoS attacks. If you experience a one terabit DDoS then it doesn’t matter if you have one server or a 100 servers, they will still be overloaded,” says Darilion.

In 2020, RcodeZero found this out the hard way after it was hit by a large DDoS targeting an encrypted email hosting service which took down its customer and internal network for a short time. Most companies would do anything to avoid talking about becoming a target, but not engineer Darilion.

For him, DDoS attacks are a technical challenge as well as an occupational hazard.

The company's local ISP mitigated the attack in Europe but could not help with the overloaded DNS servers located elsewhere in the world, leaving that job to RcodeZero DNS itself. The lesson learned was that global DDoS protection is now essential for Anycast networks, hence the decision to start using Cloudflare's Magic Transit anti-DDoS service.

"We offer 100 per cent guaranteed uptime so it's important for our service level agreements," Darilion adds. "We are very happy with this service."

A quandary for the company is where it goes next. It has a large portfolio of TLD registries which suggests that chasing enterprises is where the growth lies. However, enterprise customers have different priorities from TLDs and a growing number want DNS Anycast in conjunction with additional services such as DDoS mitigation.. Smaller enterprises also need a lot of handholding during onboarding to get the DNS configuration right.

The next ambition is to target US and UK customers. "In five years, our Anycast service will look the same as it does now. But underneath it will be a totally new service based on the open source name server platforms we use," says Darilion.

"Ten years ago, Anycast was a new feature mentioned everywhere in our marketing. Now you don't mention Anycast because if you don't have Anycast it's not a good DNS service. Now it's become implicit. Most of the customers that come to us, stay with us."

Sponsored by RcodeZero DNS.