DATASHEET

Network Design Philosophy.

For a DNS provider like NS1, the health, availability, and performance of the network is paramount. There are a number of ways in which we ensure our network is always running in an optimal state, and that starts all the way down at Layers 1 and 2 in the OSI model. In keeping with NS1's unique approach to DNS, we've also taken an unorthodox approach to building the network itself. Traditionally, DNS and SaaS businesses deploy with one or two colocation providers on several continents and then buy transit from a handful of Tier 1 ISPs.

This makes anycasting easy, but it doesn't provide much in the way of diversity, and in highly publicized cases like Netflix and YouTube it can also lead to sub-par performance because there aren't enough paths to get your bits directly to the end users.

NS1 has taken our decades of experience in the hosting industry and developed a hybrid approach where we use traditional colocation providers alongside established hosting companies who have solid networks and more interestingly, both free and paid peering agreements in place with hundreds of ISPs including valuable eyeball networks like FiOS and Comcast.

While this approach presents our NOC with more challenges than it would if we just took transit from Level 3, Cogent, Telia, and called it a day, there's tremendous upside: in addition to utilizing transit from the best Tier 1 providers in each region, we're also able to select from more than 20 smaller NSPs and 10 major peering exchanges in order to find the healthiest and fastest route available.

Today we're deployed into 26 locations around the globe with some of the best hosting and colocation providers in the industry. We're constantly working with our existing providers to optimize our routes and incorporate additional upstream providers into our blend. The result is an IP network comprised of the best transit providers on the planet that's self-healing and anycasted offering unparalleled reach, capacity, reliability, and performance to where it matters most: your end users.

Defending Against Modern DDoS Attacks.

The day to day care and feeding of our network requires constant vigilance and upkeep, but we also need to guard against malicious traffic and Distributed Denial of Service Attacks. NS1 responds to DDoS attacks with a multifaceted approach that combines a number of innovative tools and techniques (e.g. NICs with programmable FPGAs) with more traditional methods (i.e. loads of excess capacity). Here are some of the specific ways we combat the various attacks that are prevalent on today's Internet.

Basic Protocol Filtering

By virtue of the fact that NS1 is solely an authoritative DNS provider, we never expect to see any non-DNS-query traffic. This means we can filter all of our edge interfaces to reject any packets that aren't valid DNS queries. This effectively immunizes us against some of the most popular and potentially damaging attacks out there today, including DNS amplification and SNMP reflection attacks, up to line rate on our interfaces.

Overbuilding and Autoscaling

On any given day NS1 has enough infrastructure online to handle roughly 100 times our (all-time) peak query traffic. We are also deployed with several providers who offer bare-metal as a service, which enables us to rapidly (sub 30 minutes) deploy nodes as needed across nearly 10 markets, ensuring we always have ample capacity to absorb and filter attacks.

BGP Techniques

NIC-based packet filtering is extremely effective at dealing with the vast majority of attack traffic we see, however it is occasionally useful to do destination null-routing. With some of our more advanced providers we can utilize BGP flowspec in order to drop or filter traffic upstream. All of our upstreams support BGP community based null-routing.

Advanced Packet Inspection & Segmentation

Attacks that involve the abuse of real DNS records tend to have discernible patterns and we have tools that allow us to do deeper inspection of DNS packets to drop queries that we identify as likely to be malicious. Customer zones are also partitioned across a number of delivery "pools" enabling us to isolate and address many attacks at a granularity that won't impact other clients.

Super-POPs

In key markets (New York, Singapore, Virginia, Amsterdam, San Jose, and Dallas) we've built vastly over-provisioned Super-POPs that can absorb and filter massive traffic spikes. Under extreme duress we can back down one or more of our anycast announce-ments to these POPs, ensuring uninterrupted DNS delivery at the expense of a short-lived increase in latency.

Scrubbing Services

In markets where we build super-POPs, we also partner with third party scrubbing services to which we have direct cross connects. In extreme situations, we can shift our anycast announcements to these scrubbing networks and work with them to mitigate the attack traffic. This would typically only apply to extremely large attacks.

Redundant DNS

In order to achieve the utmost reliability, the largest sites on the Internet implement two DNS networks, both registered as authoritative for their domain. However, taking advantage of advanced features like load shedding or even geotargeting can be difficult or impossible due to the different ways each DNS provider implements these non-RFC features.

A lot of time and thought has gone into the design and protection of our public network, but for clients who need the utmost guarantee of uptime we recommend NS1 Dedicated DNS for the availability assurance of two separate DNS networks.

Dedicated DNS is a complete solution to the challenge of redundant DNS. Dedicated DNS is a single tenant solution deployed and managed by NS1. NS1 deploys all hardware, software and networking to deliver an anycasted DNS service dedicated to your zones and designed to meet your traffic requirements. It is deployed on separate infrastructure from the NS1 Managed DNS network. From the customer perspective, setup and management could not be any easier. Records are automatically enabled on the Dedicated network with a couple of mouse clicks on the NS1 management portal. Updates are simultaneously transferred seamlessly to all delivery nodes on both the Dedicated and Managed networks.

Monitoring, Data Feeds, Filter Chain configurations, and all other updates occur in one unified portal, providing single pane of glass management. It delivers a fully redundant, multi-network DNS without orchestration or record synchronization issues. For more information please the Dedicated DNS product page on **www.ns1.com**.