Defending Against Modern DDoS Attacks

SOLUTION BRIEF

1.855.GET.NSONE

NS1.COM

NS1 guards against malicious traffic and Distributed Denial of Service (DDoS) attacks with a multifaceted approach that combines both traditional and innovative tools and techniques. Here are some of the methodologies used to assure availability and resiliency.

NS1's Layered DDoS Protection

Resilient, Global Architecture
Designed to improve availability and decrease latency

Overbuilding & AutoScaling
Absorbs typical DDOS attacks

Advanced Inspection
Blocks known attack patterns at edge, switch and server OS.

Scrubbing Service
Redirects rare, extremely large volumetrics attacks to our partners.

Protocol Filtering
Blocks non-DNS packets at the edge to prevent popular attacks

NS1 Trex™
Near line rate filtering that withstands random Qname attacks

Super-POPs
Under extreme duress, redirects queries to vastly over-provisioned POPs in key markets

NS1.

Resilient, Global Architecture

NS1's network is designed to improve availability and decrease latency. The DNS network is built with a fully redundant architecture at 26 Tier1 POPs to meet a 100% uptime SLA. Each POP is connected to multiple Tier 1 transit providers and strategic peering relationships, which gives NS1 the capacity to absorb DDoS attacks and also decreases latency to end-user networks by orchestrating optimal routes for each region.

Protocol Filtering

All non-DNS packets are dropped at the edge interfaces of every POP. This is possible because the POPs only process DNS queries and thus there is no need to support ingress of any other protocol. This effectively immunizes the network against some of the most popular and potentially damaging attacks, including NTP amplification and SNMP reflection.

Overbuilding and Autoscaling

The NS1 DNS infrastructure is massively overbuilt so that typical DDoS attacks are simply absorbed. The platform has enough compute capacity to handle nearly 50 times nominal peak query load and hundreds of Gbps of transit capacity across 26 POPs, as well as strategic peering to further enhance internet connectivity. In a major attack, NS1 can expand the capacity rapidly by deploying DNS nameservers at several bare-metal service providers. This helps to further ensure that the infrastructure can absorb and filter all attacks.

NS1 Trex™

NS1 designed and deployed proprietary nameserver software purpose-built to provide advanced DNS services. Known as NS1 Trex™, it plays a key role in DDoS mitigation in two ways. First, it answers DNS queries extremely efficiently, thus enabling the high system-wide query capacity. Secondly, it implements a memory architecture that enables near line rate filtering.

Historically, random Qname attacks have been extremely impactful to authoritative DNS services. This attack involves sending a high volume of DNS queries to a made-up hostname under a valid domain name. For example, if a DNS service hosts example.com, the attacker would send DNS queries for abcd.example.com, fgf.example.com, etc.. This crushes the typical name server.

NS1 designed Trex to withstand this type of attack easily. By storing all zones in shared memory and implementing a super-fast lookup algorithm, Trex can respond with a non-existent domain (NXD) response immediately and with little impact to system capacity.

Advanced Inspection

Most DDoS attacks against DNS have a discernable pattern that can be filtered. For example, the attack may be to specific domain names, have incorrect flags set in the DNS header, or may be from bogon address space (e.g. private IP addresses). NS1 utilizes advanced tools to recognize these discernible patterns and drop those identified to be malicious. NS1 POPs implement filtering at multiple layers, including at the edge router, switch, and server operating system. For DNS queries that make it through the other filter layers, Trex can rapidly filter the queries based on complex patterns with little impact to its ability to answer legitimate queries.

Super-POPs

In key markets (New York, Singapore, Amsterdam, San Jose, Dallas, and Washington DC) NS1 has built vastly over-provisioned Super-POPs that can absorb and filter massive traffic spikes. Under extreme duress, DNS queries can be redirected to these Super-POPs, thereby ensuring uninterrupted DNS delivery at the expense of a short-lived increase in latency. Traffic can be rate limited and tunneled back to smaller POPs to add extra compute capacity.

Scrubbing Service

In the case of extremely large volumetric attacks, NS1 can shift Anycast announcements to a commercial DDoS mitigation service and work with them to mitigate the attack traffic. Given all of the other tools at our disposal, NS1 rarely needs to resort to this step, however, having this capability ensures that NS1's managed services can handle the largest possible DDoS attacks without missing a beat.