DNSSEC: DNS Security Without Compromises.

Many organizations have held back from using DNSSEC because doing so meant giving up the DNS traffic management capabilities they rely on to deliver high quality online services. It does not have to be that way. With NS1, you can use all the advanced traffic management capabilities of our platform on your DNSSEC signed zones. Security without compromises.

NS1.

DNSSEC Feature Brief

The Domain Name System Security Extensions (DNSSEC) prevent attacks that can compromise the integrity of answers to DNS queries. When successful, such attacks can result in users being falsely directed to bogus websites masquerading as legitimate sites, or can be used as a form of denial of service.

Although attacks on the integrity of DNS information can have serious consequences, many organizations have not protected their zones with DNSSEC. Technical barriers to using DNSSEC have resulted in an unfortunate trade-off between functionality and security. Mindful of these issues, NS1 has implemented DNSSEC to break down the technical barriers, eliminating the need to choose between functionality and security.

DNSSEC and Traffic Management

DNS traffic management has become a staple for organizations of all sizes. Small organizations and enterprises alike have come to rely on traffic management capabilities that range from the relatively basic, such as:

- Monitor your sites and don't send users to a site that is currently down
- Geo routing – send users to the closest point of presence

To advanced:

- Route users to the best performing, most cost effective CDN
- Use real time load telemetry to balance traffic between multiple data centers

Unfortunately, DNSSEC implementations on standard DNS platforms and on most DNS managed services are incompatible with traffic management. DNSSEC "breaks" even basic functions such as georouting. It is often the case that the most important zones – the ones you should secure with DNSSEC - are the very same ones where traffic management is most valuable. The trade-off is security versus the quality of your online services.

NS1 has solved this dilemma. We deliver DNSSEC without the compromises and trade-offs enterprises have been struggling with. All of NS1's advanced traffic management capabilities are available on DNSSEC signed zones. This includes our suite of metadata, data feeds, and filter chain. Configuring and managing advanced traffic management on DNSSEC signed zones is no different from unsigned zones. It all "just works." Configure your zones, records and traffic management as needed to meet your performance and business objectives, apply DNSSEC with a mouse-click (or API call), and your signed zones are ready to go.

Redundant DNS and DNSSEC

DNSSEC helps protect the integrity and authenticity of your DNS records. It prevents man-in-the-middle attacks from corrupting information on DNS resolvers (so called "cache poisoning"). However, DNSSEC does not protect the availability of DNS systems. The need for redundancy in your DNS is as great with DNSSEC as without. Some would argue the need is even greater.

A dual provider DNS infrastructure where both providers support DNSSEC does provide availability assurance. This comes at the expense of traffic management. While many enterprises have managed to get basic DNS traffic routing to work in dual provider set-ups, once they enable DNSSEC those capabilities are lost.

NS1's Managed DNS combined with Turnkey Dedicated DNS provides redundancy and full featured traffic management for all your DNSSEC signed zones. All zones and records are managed on your NS1 portal interface or through API. There is no need to deal with record synchronization issues and complexities of zone transfers. The zones and records are managed in one place. Updates to your zones are propagated to our globally anycasted DNS servers and your Dedicated DNS servers in seconds.

FEATURES AND CAPABILITIES

✓	Compliant with DNSSEC RFCs.
✓	Advanced traffic management supported on signed zones.
✓	Uses high performance elliptic curve cryptographic algorithms. No impact on DNS response time.
✓	Support for redundant DNS set-ups, with advanced traffic management.
✓	Support for Dual Provider configurations (NS1 as Secondary DNS). Advanced traffic management not supported in Dual Provider mode.
✓	Easy configuration and management.
✓	Available with all Managed DNS Developer and Enterprise plans.