The Only Secondary Network You Need – UltraDNS²

A company's on-line presence is critical in defining that customer's brand. Whether it is your website, e-commerce site, service portal, gaming server, SaaS application or any other internet facing services, your business is defined by the experience that you give your users.

To compete, your sites need to be available at all times, fast to respond, and secure with your customer's data. DNS resolution is one of the essential components to ensure a flawless internet experience for users as it is the means by which customers can find your on-line services. Because of this reliance, it is important for customers to include authoritative DNS resolution as part of their business continuity/disaster recovery planning and consider implementing redundant networks for this critical function.

Over the past few years alone, a number of the well-known DNS providers have experienced extended outages due to a variety of different issues including software malfunctions, routing issues, and operational errors. The most common source of issues has been distributed denial of service (DDoS) attacks. On October 21, 2016, a well-known managed domain name system (DNS) provider was rocked by a massive, distributed denial-of-service (DDoS) attack. The attack not only suspended the availability and services of the DNS provider, but the collateral damage was also spread to several well-known brands whose websites and applications also suffered intermittent outages. Today, cybersecurity experts are now preparing not for an "if" but "when" an attack happens. They want to ensure their network is protected to detect an attack and to be able to mitigate it quickly without interruption to their services and, of course, their customers.

Redundancy is Key

The single most important thing that organizations can do to protect their authoritative DNS service is to implement redundant DNS solutions. In the wake of the Mirai botnet attacks, industry analysts (e.g. Gartner) recommend that organizations have a secondary DNS network for better security, redundancy and availability. It's not about having a Plan B if your Plan A fails. It's about having a smarter Plan A that provides redundancy of your DNS traffic between two trusted networks. This strategy protects your brand from a single, take-down DDoS attack, operational mishaps, and isolates you from impact from software defects. Neustar Security Services UltraDNS² was developed with this in mind.

Introducing UltraDNS²

Neustar Security Services UltraDNS² combines the award winning UltraDNS resolution network with a second global DNS anycast network to provide exponential value. UltraDNS² is hosted, and the network operated, by a leading anycast cloud provider with different network operations from the underlying systems, provisioning, automation, routing policies, and transit providers than UltraDNS. This offers you the redundancy of having a distinct second network provider with all the advanced features and functionality of UltraDNS. With UltraDNS², you gain a single pane of glass management that allows you to easily manage your DNS records across both networks. Having one provider for both your networks provides a lower total cost of ownership, providing one point of contact for managing your DNS network. UltraDNS² puts you in the best position to ensure your online presence is uninterrupted.

BENEFITS

- Advanced features across both networks
- Exclusive offering to a select group of premier customers
- Achieve business continuity and disaster recovery goals
- Single pane of glass management of both networks
- Lower total cost of ownership
- Dedicated 24x7x365 support

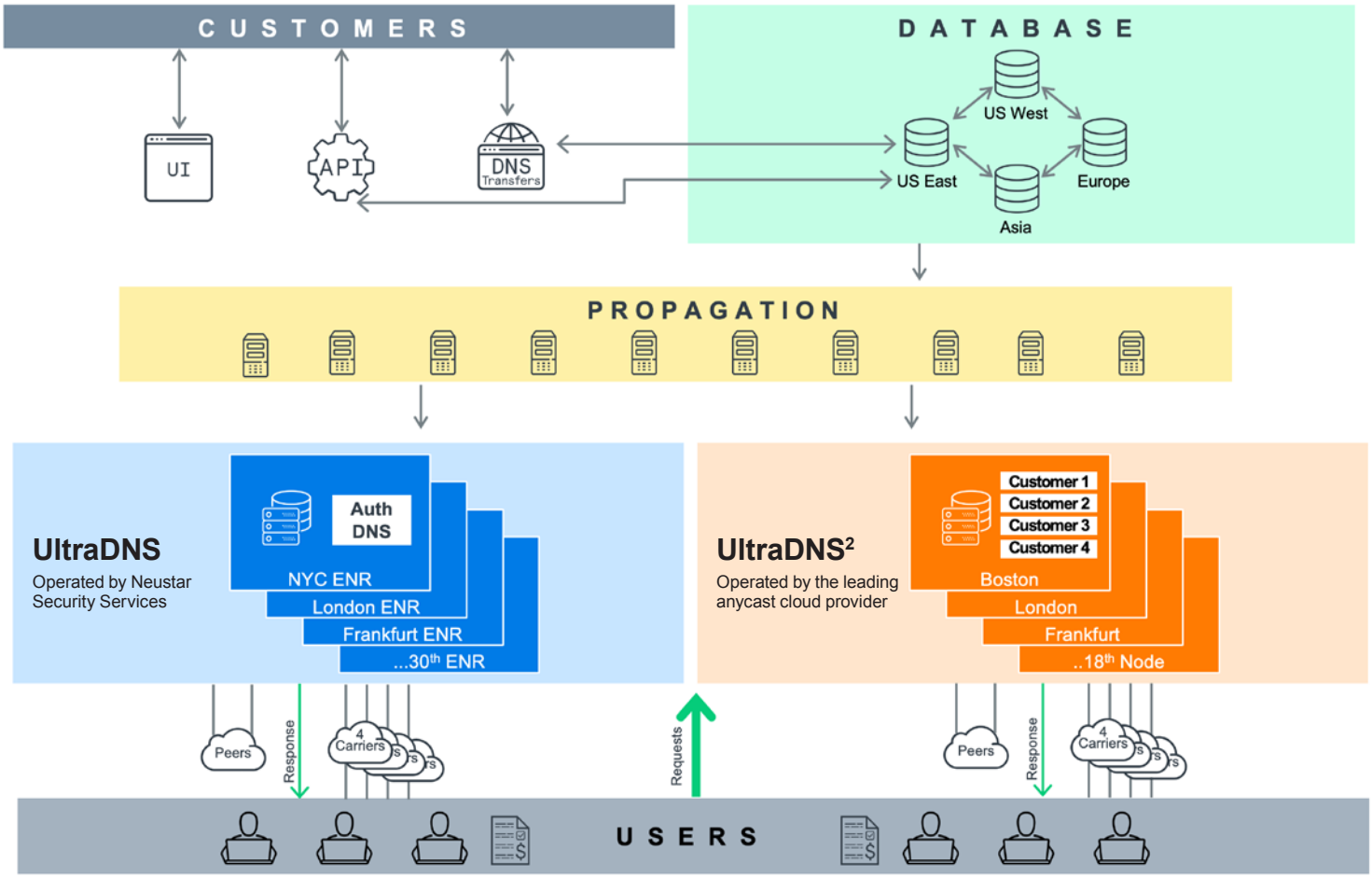
FEATURES

- Distinct anycast network and routing policies
- Additional 18 nodes globally
- Diverse network operations
- Isolated edge server operations
- DDoS mitigation by UltraDDoS Protect
- Option to have isolated nameservers on the UltraDNS² network

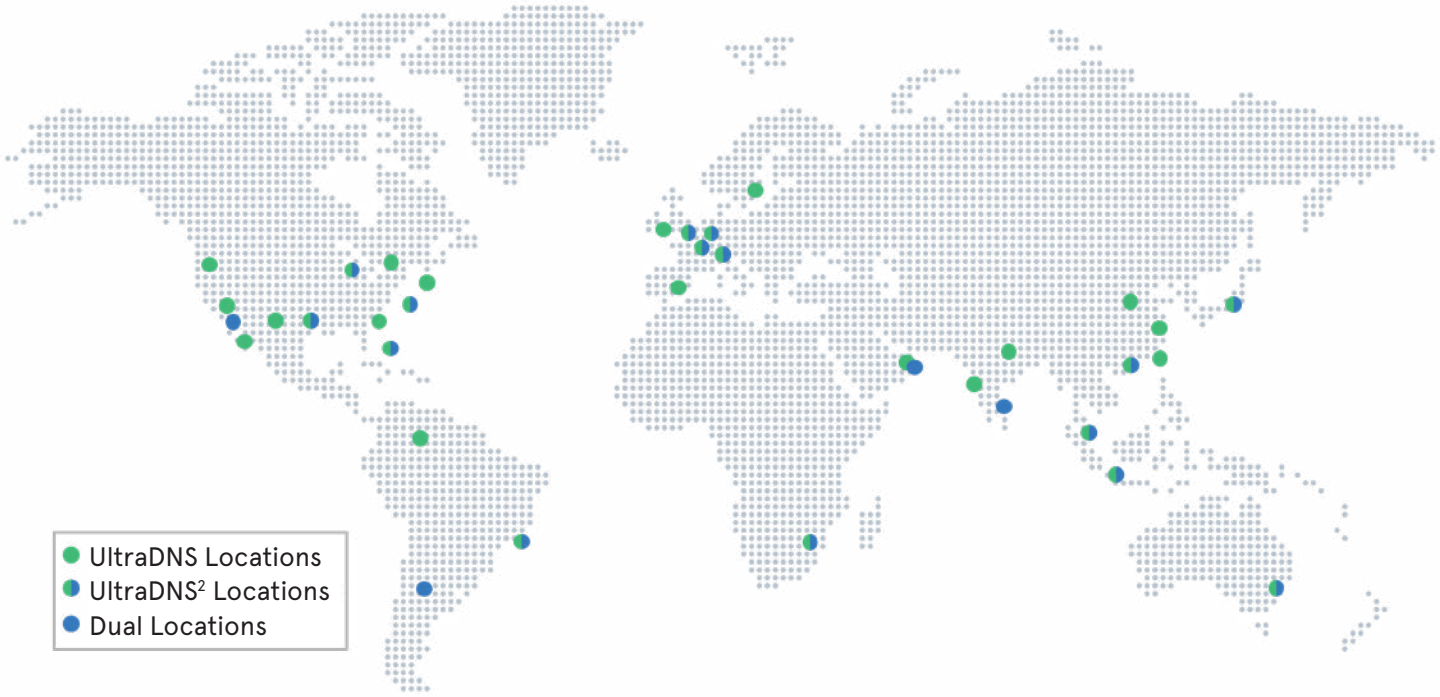
UltraDNS² and UltraDNS Platform Comparison Table

AREA OF OPERATION	SIMILARITIES	DIFFERENCES	BENEFITS
Network and transit	Global footprint, Anycast operation, and multiple transit options per location	Different hosting partners, physical locations, transit providers	Higher geographic and transit redundancy increases resilience and lowers risks associated with network events
Network operations	Dedicated and experienced network teams	Independent teams for UltraDNS²	Additional expertise, increased operational resilience
Nameservers and resolvers	Proven UltraDNS code base, multiple nameservers per customer, vanity nameserver support, IPv4 and IPV6 resolution	UltraDNS² provides the option of isolated nameservers per customer	Eliminates "noisy neighbor" issues and significantly reduces risk of collateral damage due to attacks on other customers
Zone management, billing and reporting	Single pane of glass across both networks	Different network paths for zone propagation. Common management UI and reporting	Simplicity lowers management burden. Eliminates the need/risk of developing a workload management tool
Feature/functionality	All features are available across both networks	N/A	Reduces complexity and creates a better customer experience

UltraDNS² Network Overview



UltraDNS and UltraDNS² Coverage Map



UltraDNS Nodes

ASIA	EUROPE	NORTH AMERICA	SOUTH AMERICA	MIDDLE EAST	AFRICA	OCEANIA
Beijing Mumbai Hong Kong Shanghai Singapore Taipei Tokyo	London Amsterdam Paris Frankfurt Dublin Madrid Stockholm	Dallas Chicago Ashburn Miami Los Angeles Phoenix San Jose Seattle Atlanta New York Toronto	Sao Paulo Colombia	Fujairah	Johannesburg	Sydney

UltraDNS² Nodes

ASIA	EUROPE	NORTH AMERICA	SOUTH AMERICA	MIDDLE EAST	AFRICA	OCEANIA
Chennai Singapore Hong Kong Tokyo	London Amsterdam Paris Frankfurt	Seattle Sunnyvale Dallas Ashburn Miami	Santiago Sao Paulo	Dubai	Johannesburg	Sydney

Find out how UltraDNS² can work for you.

TO LEARN MORE CONTACT US

Visit: www.neustarsecurityservices.com
Call USA: +1 (844) 929-0808
Call EMEA: +44 808 175 1189

SS-DNS-J93755-05.24.2022