Dyn

WHITEPAPER:

Extending Global Load Balancing to the Cloud with Secondary DNS

Extending Global Load Balancing to the Cloud with Secondary DNS

Introduction

The fast-evolving digital landscape is changing the game for all organizations. The way we consume content, conduct research, consume video and music, and drive efficiency in our work environment is raising the bar for digital experience. Organizations that rely on the internet to reach customers and drive revenue increasingly turn to cloud-based infrastructure and content delivery networks (CDNs) to achieve the reach and global footprint needed to keep up with customer demands. Delivering these services with high availability and performance across an unpredictable internet over which you have very little visibility and control is a major challenge.

Internet Performance Management (IPM) addresses these new challenges by providing a complete end-to-end view of the internet and the infrastructure locations end users connect with as they interact with brands online. While some organizations have already adopted online strategies that enable them to take advantage of the best cloud providers and CDNs to reach each of their target markets, many others are just starting this process.

So how can organizations adapt on-premise global load balancing (GLB) infrastructure for today's internet challenges? The most logical first step is adding a cloud-based secondary DNS solution that complements existing GLB. This approach immediately extends global reach, increasing resiliency, and improving end user performance across the globe. This whitepaper explores the benefits many organizations are achieving by combining their existing GLB services with a cloud-based secondary DNS solution.

IPM: The Global Load Balancing Approach

Whether you're serving customers, partners, or internal users through two data centers or twenty, supporting just a few applications or many, you want all users to have the best experience. Fast performance and availability are crucial to such an experience— and real, efficient GLB is a key step towards delivering this experience.

While most organizations have invested in improving the performance and resiliency of their on-premise GLB capabilities, very few organizations are able to achieve the level of performance and high availability that a cloud-based anycast DNS network can offer. This is why enterprises across the globe have begun complementing their existing GLB capabilities with a secondary DNS service that operates in an always-on (active-active) manner to respond to incoming DNS requests. This approach provides an added layer of resiliency against outages and malicious attacks at the DNS layer.

TERM DEFINED

GLOBAL LOAD BALANCING

The practice of intelligently distributing Internet website or application traffic across multiple data centers and cloud service providers for optimal peformance and 24/7 availability.

The primary role improved online performance and resiliency play in the success and growth of a business is undeniable:

- **Maintain Availability:** Uptime is the watchword of IT infrastructure and operations professionals - and for good reason. A recent global benchmark study found 90% of respondents indicated service availability is highly critical to their customers (at least 8 on a scale of 1-10)[1].

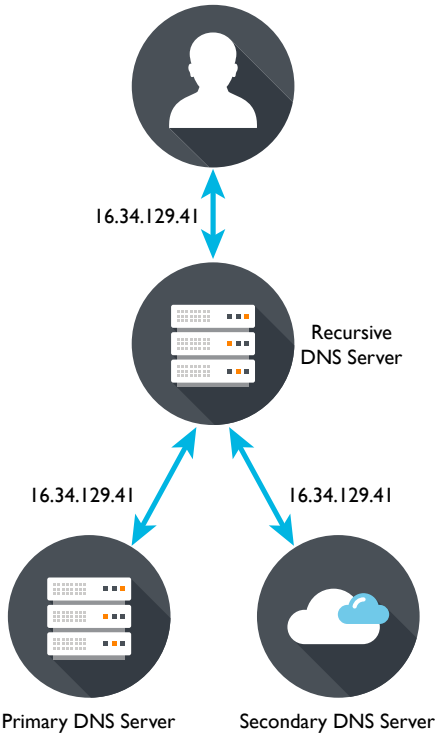
[1] "2014 Service Availability Benchmark Survey," Continuity Software, 2014.

- **Improve Digital Experience:** Consistency matters when building brand. The first impression customers have of your business will be greatly influenced by the performance of your web pages and applications, especially when you think globally. Forrester Research has observed that emerging markets, with areas of vastly different network quality (even within urban areas), have notoriously poor consistency[2].
- **Improve Time-to-Resolution:** Improving incident resolution time can significantly improve operational efficiency. Of course, the most quickly resolved incident is the one that doesn't occur in the first place!

In short, effective management and balancing of the internet traffic to and from your data centers and cloud service providers has become critical to growing enterprise ecommerce revenue, serving customers, and empowering employee productivity.

Secondary DNS: Extending GLB to the Cloud

The goal of global load balancing is to get users to an available data center or cloud provider that will deliver the best performance every time. By adding a secondary DNS service as a redundant complement to your GLB appliances, end users are directed to these locations faster and the risk of having requests go unanswered is avoided.



Secondary DNS operates in an "always on" manner to complement your existing infrastructure as an additional authoritative DNS service. When an end user's recursive server initiates a DNS request, both your existing GLB appliances and the secondary DNS service will respond as soon as they receive the request. Whichever response reaches the recursive server first will be passed back to the end user, completing their request.

This process effectively creates a race to respond to each incoming DNS request, ensuring performance will only improve. All domain information will continue to be configured on-premise in the same manner in which it's managed today. This information will then be synchronized with the secondary service (using one of several industry supported protocols) to ensure both solutions are returning the same information to end users.

Secondary DNS reduces the risk of outages to critical services while also protecting against delays in connecting users to these services as any degradation on either the secondary service or the on-premise solution will simply result in the alternative service winning the majority of the races to respond to incoming requests.

A cloud-based service is also in a position to constantly check end-to-end system availability in the data centers simultaneously, and from multiple locations, before it directs traffic to the site.

Flexibility = More Control With Less Effort

In order to ensure the highest performance to all end users across the globe, your global load balancing capabilities must be highly flexible to react to changing circumstances that may affect your applications and services. Adding a cloud-based secondary DNS service to your GLB infrastructure allows you to quickly adapt to dynamic traffic flows far more easily and cost effectively than relying solely on your on-premise infrastructure. And with the redundancies designed into their distributed network topologies, established service providers represent little risk—all of which gives you more control to quickly and confidently accommodate any changes to your infrastructure as future demands lead to even more distributed services.

[2] "Making Global ECommerce Trends Work: Forrester Offers Advice," MadMobile news, January 28, 2013.

Utilizing a global DNS provider in your infrastructure immediately expands your online footprint to each corner of the globe. This gives organizations the agility to expand into global markets as business warrants, without the need to build out and maintain costly data centers to serve those new markets.

Availability And Performance: The Anycast Network Experience

When you engage with any service provider, you don't just leverage their infrastructure, but their expertise as well. The most experienced managed DNS providers have designed and maintain global networks for the rapid and reliable DNS resolution through the use of anycast networks. Different than unicast topologies, upon which GLB appliances typically rely, anycast networks provide a one-to-many relationship between IP addresses and their associated nameservers. The service provider, rather than the customer, makes the investment in time and expertise required to set up and maintain an anycast network—an on-going investment that would be prohibitive for all but the largest enterprises.

Anycast networks protect availability, achieving high redundancy and reducing risk of service interruption by distributing DNS service for each IP address across multiple nameservers strategically placed throughout the world. If a single nameserver goes down (whether from hardware failure or DDoS attack), that server will automatically be removed from the available routing options, and future traffic will continue to be routed to the remaining nameservers. Once service to the nameserver is restored, it can be reactivated on the network.

Distributed DNS networks can be implemented using two distinct standards-based IP addressing schemes: unicast addressing or anycast addressing.

The unicast approach is far simpler to implement, but the anycast approach offers significant performance & resiliency advantages.

Distributed Denial of Service (DDoS) attacks are one of the biggest risks faced by enterprise IT teams. Some companies purchase GLB appliances to protect against application-level attacks—but DNS layer DDoS attacks are very different. Given its vantage point serving a global customer base, global internet Performance Management providers offer an extremely high level of expertise in DDoS protection—and the staff to perform a level of monitoring that is beyond most companies' IT teams.

The average cost of a single DDoS outage is $882K.

Source: Ponemon Group

What About Visibility?

It might seem that an on-premises appliance would provide a greater level of visibility on traffic. Certainly when it comes to traffic information, on-premise GLB appliances connected to local load balancers from the same vendor can provide greater detail on sessions after connections have been resolved and conditions within the data center itself.

They do not, however, provide broader, internet-level visibility of what's impacting end users across the internet. Managing traffic outside enterprise perimeters, including between data centers, involves the architecture and protocols of the internet—visibility you cannot get from an on-premises solution in the way you can get from an internet-based service provider.

Through portals with intuitive GUIs and APIs that let you automate your everyday processes, cloud- based services can make it easy to monitor online traffic far more effectively and make adjustments to traffic policies when needed. Experienced service providers may also share additional information that helps you monitor the impact of the internet on your business, through sensor grids, global geolocation analysis, and real-time internet connection mapping. Given the perspective of the service provider, you'll know a lot more about what's happening elsewhere on the internet that will help you make better decisions about your application traffic and infrastructure planning.

Conclusion

No one questions that the scale, complexity and volatility of the internet is on the rise. There are currently over three billion global internet user, while trends like agile application development and the internet of things (IOT) compound internet growth. In the meantime, internet threats are also increasing, with a seemingly unrelenting volume of DDoS, route hijacks and other security threats. These dynamics not only make clear that GLB is imperative, but also that secondary DNS as part of an internet performance management (IPM) strategy is critical to maintaining business continuity and delivering superior digital experience to end users.

About Dyn

Dyn is the Internet Performance Management (IPM) company, giving IT organizations the power to manage the internet like they own it. Dyn helps everyone from high-growth startups to global leaders like Pfizer, Visa, Netflix and Twitter solve the challenges associated with rising internet scale, complexity and volatility. The Dyn IPM platform combines the world's most advanced DNS with real-time global internet monitoring, allowing organizations to monitor and control how users connect with their online services.

learn more

To learn more about how secondary DNS can help your internet performance, please visit: dyn.com/secondary-dns