WHITE PAPER

Designing DNS for Availability and Resilience Against DDoS Attacks

Introduction

Edge DNS provides organizations with an authoritative DNS service to connect end users with their websites and other applications. While much attention is paid to performance, organizations often overlook the importance of availability and resilience for DNS – especially against DDoS attacks that seek to disrupt the service and prevent end users from connecting. Akamai designed Edge DNS to remain available through the largest DDoS attacks, with unmatched global scale, a segmented IP Anycast architecture, and multiple DDoS controls, including the ability to leverage other Akamai services when necessary. Offered as a managed DNS service, Edge DNS provides an optimal combination of performance and availability to always connect organizations with their end users.

Note on Statistics

Akamai originally built Edge DNS to provide authoritative DNS services in support of its global content delivery network (CDN) solutions. Over the years, Akamai has learned many lessons on how best to scale and keep available such a large DNS infrastructure. The high-level statistics to the right provide a general sense of the scale of the platform. However, statistics alone cannot provide meaningful guidance on availability and resilience, and should be considered along with the platform architecture, specific DDoS mitigation capabilities, and the overall capacity available to Akamai when protecting the platform from attacks.

Platform statistics

- Thousands of name servers
- 1,000+ points of presence
- 140+ cities
- 40+ countries

Note that Akamai does not disclose specific details on the number of name servers or numbers, locations, or sizes of our points of presence for security reasons. This policy protects both Akamai and our customers from attackers who may attempt to use that information when planning attacks.

Architecture

As you can see from the statistics above, Edge DNS has greater scale than most competing authoritative DNS services in the market today. However, high-level statistics on the number of servers and points of presence, or the amount of total network capacity, are insufficient to understand the level of availability and resiliency for a global platform. Unlike other DNS solutions that have traditionally focused exclusively on performance, Akamai specifically architected Edge DNS for availability and resiliency against DDoS attacks, in addition to performance, with architectural redundancies at multiple levels, including name servers, points of presence, networks, and even segmented IP Anycast clouds.

IP Anycast

Edge DNS comprises thousands of name servers deployed in more than 1,000 points of presence employing an IP Anycast model to respond to DNS queries. IP Anycast directs queries from end users to the closest point of presence for resolution. Along with faster performance, IP Anycast provides several fundamental benefits for availability and resiliency, which is why most authoritative DNS services use it:

- **Availability** – IP Anycast allows name servers in different network locations to respond to queries made to a single IP address. By leveraging IP Anycast, Edge DNS not only provides organizations with DNS resolution in multiple data centers, but also improves availability by distributing load globally. In addition, individual physical servers or entire points of presence can go offline without impacting the overall ability of a domain's resolution.
- **Scale** – Comprising many physical servers across numerous points of presence, the Edge DNS infrastructure provides organizations with significant computing resources that they can consistently rely on when responding to large volumes of DNS requests. Edge DNS also has access to significant additional network capacity in many of its points of presence, as it often shares capacity with other Akamai services. This affords Edge DNS much greater scale to respond to DNS floods and other forms of DDoS attacks than a standalone DNS service.
- **Distribution** – Beyond enabling greater scale, IP Anycast allows Edge DNS to distribute traffic across multiple points of presence and diverse network locations. Thoughtful consideration of the geographic locations and network deployments for these points of presence can help contain the impact of smaller attacks to specific geographies or networks and preserve availability for client systems in other areas.

Leveraging IP Anycast is not unique to Akamai. By allowing multiple name servers to resolve DNS queries from end users, IP Anycast improves the availability of name resolution for any DNS service. But even with IP Anycast, resiliency remains limited by a platform's total scale, and large DDoS attacks can still overwhelm a cloud-based platform. What's more, without a diverse architecture, even smaller attacks have the potential to take down DNS services in specific geographical regions, rendering them unavailable for large numbers of end users and impacting the availability of any websites to which those users connect.

Edge DNS Clouds

To further improve its resiliency against attack, Edge DNS segments its name servers and points of presence into multiple IP Anycast clouds. An Edge DNS cloud consists of dedicated name servers and points of presence along with associated network capacity and connectivity. Every cloud operates independently of one another, and Edge DNS can be equivalent to multiple standalone DNS providers, in terms of availability, scale, and distribution.

Edge DNS IP Anycast clouds represent a diverse set of architectures. While no two clouds are identical, they broadly align with two design principles – performance and availability:

- **Performance** – A performance cloud can have more than 100 points of presence distributed around the world, each consisting of a set of name servers. As shown in Figure 1, a performance cloud deploys small clusters of name servers in many locations closer to end users and local Internet Service Providers (ISPs) in order to provide faster lookup times and better raw performance. The trade-off is that small points of presence offer less resilience to DDoS attacks by definition, with fewer compute resources and less network capacity.
- **Availability** – Edge DNS maintains many availability clouds. As shown in Figure 1, availability clouds have fewer points of presence but include one or more anchor regions that can comprise hundreds of name servers in a centralized data center with a large amount of dedicated network capacity and connectivity through multiple networks. The anchor region provides the availability cloud with the scale to respond to large spikes in DNS requests and other network traffic. Availability clouds augment anchor regions with a small number of smaller points of presence to maintain an acceptable level of performance for users around the world.

Figure 1: Edge DNS combines multiple DNS clouds with different architectures to offer an optimal combination of performance, availability, and resiliency against DDoS attacks.

Segmented Architecture

Edge DNS offers a fundamentally different degree of availability compared with other providers operating authoritative DNS services on a single IP Anycast cloud. For all providers, IP Anycast provides some availability benefit by allowing the service to maintain overall uptime through smaller attacks that may only impact specific geographies rather than the entire platform. However, even localized outages will impact end users in affected geographies as well as organizations relying on that service to connect with those users. In addition, larger DDoS attacks with traffic generated by attacking systems around the world have the potential to cause an outage of the entire platform.

With numerous and diverse IP Anycast clouds, Edge DNS can continue functioning even with the loss of one or more clouds. This provides a higher degree of availability and resiliency against DDoS attacks when compared with a single cloud architecture. In addition, operating multiple IP Anycast clouds

offers the advantage of segmenting traffic across subsections of the overall platform in order to mitigate the impact of even massive DDoS attacks. For example, an attack against a single Edge DNS IP Anycast cloud will be directed at the physical name servers and points of presence that compose that specific cloud. The segmented architecture isolates the impact from other IP Anycast clouds, allowing Edge DNS to maintain platform availability in all geographies, even though individual clouds or customers may be under DDoS attack.

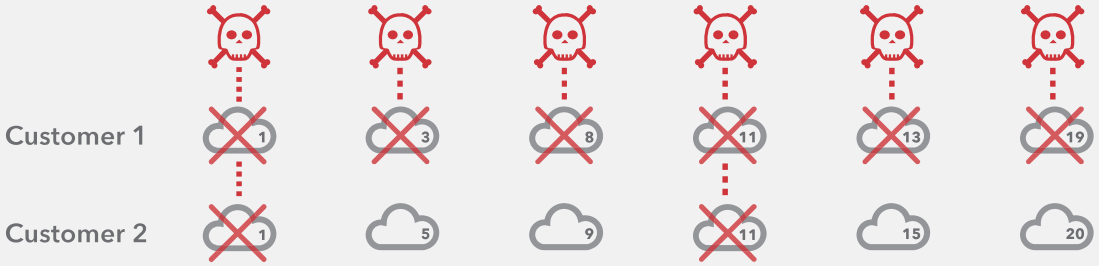

Figure 2: Every Edge DNS customer receives name servers on a unique combination of performance and availability clouds, minimizing the collateral damage from an attack against other customers.

In addition to increasing overall platform resiliency, Edge DNS segmented architecture also mitigates the risk of collateral damage for individual customers when name servers utilized by other customers are attacked. Edge DNS assigns every customer multiple Edge DNS clouds — and in a unique combination of performance and availability clouds not shared by any other customer. As shown in Figure 2, this distribution minimizes the overlap in name servers and IP Anycast clouds between any two customers. It also ensures that every customer will have name servers that are available even when IP Anycast clouds assigned to another customer are specifically targeted by a large DDoS attack.

Managing Customer Delegations

Multiple DDoS attacks against a single organization often take place over longer periods, and Akamai has seen broad and sustained attack campaigns extend for months or more in duration. In this situation, the segmented architecture of Edge DNS affords Akamai greater flexibility in further minimizing the impact on customers that are not targeted by the attack. As shown in Figure 3, Akamai can reassign an individual customer's clouds and further isolate the impact of an attack when necessary.

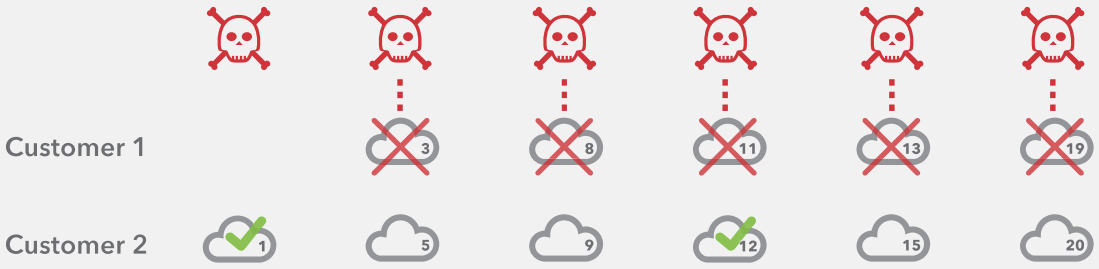

Figure 3: Akamai can manage name server delegations to further minimize the impact of an attack (compared with Figure 2, above), such as by moving a targeted customer off of an individual cloud and minimizing the overlap for nontargeted customers.

- **Move a targeted customer off a specific cloud** – Every Edge DNS customer shares IP Anycast clouds with other customers. As a result, an attack that targets all of one customer's Edge DNS clouds can impact the availability of clouds also assigned to other customers. Under normal circumstances, recursive resolvers automatically switch to better-performing clouds, but for sustained campaigns, Akamai can reassign the IP Anycast clouds of the targeted customer to restore availability for nontargeted customers.
- **Minimize overlap for nontargeted customers** – Occasionally, multiple Edge DNS customers may share a higher-than-normal number of Edge DNS clouds. In this situation, it is possible that a massive attack against a single customer can have a measurable performance impact on other customers despite the overall service remaining available. When necessary, Akamai can reassign the clouds for nontargeted customers to reduce or eliminate the overlap with the targeted customer and restore performance for their end users.

Diverse Server Deployments

Within each Anycast cloud, Akamai deploys physical name servers in different locations designed to increase the overall resiliency of that cloud. Diverse Edge DNS cloud locations provide another layer of segmenting traffic among different networks in order to maximize availability in different circumstances. For example:

- **In data centers with multiple networks** – When considering resiliency against DDoS attacks, the diversity of network connectivity can be as important as the amount of capacity. Large DDoS attacks can overwhelm upstream ISPs and other networks before reaching a data center, causing network congestion and service outages even if the data center itself remains unaffected. To preserve availability and its ability to respond to DNS queries from end users during attacks, Edge DNS deploys name servers into large data centers with not only large amounts of capacity but also connectivity through multiple networks.
- **ISP isolation** – In many cases, Edge DNS deploys clusters of name servers directly in the networks of individual ISPs. These name servers often broadcast their IP Anycast traffic only within those networks and resolve DNS queries only for end users of those ISPs. While this arrangement limits the number of end users that any specific cluster of name servers can serve, it also preserves availability for those users when an IP Anycast cloud is targeted by an attack outside that ISP. An attacker would have to have systems on that specific ISP's network in order to see those name servers, and even then, the available capacity is often enough to protect that one cloud.
- **Network diversity** – Customers are intentionally assigned diverse clouds – some with server locations unique to specific ISPs and some with a broader range of connecting machines. This architecture ensures that the recursive name servers of a given client will always be able to connect to an available Edge DNS cloud.

- **In data centers shared with other Akamai services** – Operating many different services beyond authoritative DNS, Akamai can deploy Edge DNS name servers into data centers that support multiple services. As discussed in more detail below, this affords Edge DNS access to a larger amount of network capacity when responding to large DDoS attacks – both dedicated network capacity as well as public peering arrangements that Akamai already has in place for other services.

DDoS Controls

Beyond its architectural design, Edge DNS includes several controls to help mitigate the impact of a category of DDoS attacks known as DNS floods. While many DDoS attacks use a large amount of traffic to overwhelm network links, DNS floods generate large volumes of legitimate DNS requests to consume compute and memory resources on physical name servers and prevent them from responding to queries from actual end users. Akamai protects the Edge DNS platform against DNS floods in several ways:

- **Scale** – The scale of Akamai's authoritative DNS service can be several times that of other competing DNS solutions. Edge DNS utilizes thousands of name servers deployed in more than 1,000 points of presence around the world. While not specifically a DDoS control, IP Anycast distributes attack traffic across geographies and networks, while the number of physical name servers provides Edge DNS with sufficient compute and memory resources necessary to absorb large spikes in DNS requests.
- **Rate limiting** – Edge DNS includes rate limiting capabilities and can automatically drop requests from individual IP addresses after the volume of requests exceeds a set threshold. Rate limiting prevents large spikes in DNS requests from consuming compute and memory resources on physical name servers and can be useful when responding to attacks that generate a high volume of requests but consume relatively low bandwidth. Note that the rate limiting capabilities on Edge DNS are not configurable by customers, but employed by algorithms unique to the Edge DNS platform.
- **DNS white-listing** – Because of its position on the Internet, Akamai has unique visibility into the behavior of recursive resolvers responsible for approximately 95% of legitimate DNS lookups on the Internet. When necessary under heavy load, Edge DNS can employ a positive security model and restrict DNS requests to a list of known-good DNS resolvers.

Regarding Capacity

While DDoS controls can be useful in mitigating the impact of DNS floods, other types of network-layer DDoS attacks require having sufficient available network capacity to absorb the high volume of traffic. The risk of volumetric attacks has increased dramatically over the past several years, with the largest known attacks now far exceeding 1 Tbps in peak bandwidth.

Akamai does not disclose the amount of capacity of the Edge DNS platform in order to avoid providing attackers with a quantifiable target. However, Akamai continuously invests in every aspect of platform scale, growing the Edge DNS infrastructure to keep pace with new customers and traffic growth on the Internet. As a cloud service provider, Akamai can rapidly repurpose servers and deploy DNS capacity into new regions. Akamai maintains a significant amount of available capacity to absorb large spikes in traffic, with normal traffic on the Edge DNS platform consuming less than 1% of its overall capacity. If necessary, Edge DNS can also leverage resources from other Akamai platforms to mitigate DDoS attacks.

Leveraging Other Akamai Platforms

The traditional method of using network capacity to estimate the ability to withstand a high-bandwidth DDoS attack does not work with Edge DNS — primarily because Edge DNS can leverage resources from other Akamai platforms. More than just a DNS company, Akamai operates many services besides Edge DNS. Of all the services that Akamai operates, authoritative DNS is critical to the operation of other services, but remains small in terms of overall traffic. This offers several opportunities to augment the capacity available to Edge DNS when needed:

- **Borrowing capacity from the CDN** — In many cases, Edge DNS deploys name servers within the same points of presence as servers belonging to other Akamai services running on the Akamai CDN. These points of presence are often significantly larger, as they are designed to support services that consume much higher bandwidth. This also affords Akamai the operational flexibility to borrow capacity from the CDN when necessary, by diverting other services through other Akamai points of presence and making shared network capacity available exclusively to Edge DNS so it can absorb large DDoS attacks.
- **Deploying dedicated mitigation capacity** — In addition to authoritative DNS and CDN, Akamai operates a separate DDoS protection service with dedicated mitigation capacity and capabilities. When necessary to mitigate large DDoS attacks, Akamai can assign individual name server delegations through its Prolexic scrubbing centers to leverage that dedicated capacity and DDoS mitigation tools. This effectively deploys the DDoS mitigation capabilities of the Prolexic platform in front of Edge DNS, preserving the resources of Edge DNS to respond to legitimate queries from end users.

Multiple DNS Vendors

Edge DNS offers an authoritative DNS service with several times the scale of many competing services, a resilient architecture with numerous segmented IP Anycast clouds, and the ability to leverage the additional capacity and capabilities of other Akamai services to protect it from DDoS attacks. With these advantages, Edge DNS can provide the availability and resiliency required to operate as an organization's sole authoritative DNS provider. However, some organizations may choose to deploy Edge DNS alongside their existing solution. A multivendor deployment allows organizations to maintain their existing DNS records management practices while supplementing their primary DNS solution with the additional availability and redundancy of Edge DNS.

Deployment Options

Edge DNS supports several options for deploying Edge DNS in a multivendor environment:

- **Traditional secondary** – Organizations with an existing DNS provider can deploy Edge DNS as a secondary service to augment their primary DNS solution. Organizations continue managing their DNS records with their primary provider and use zone transfers or Edge DNS APIs to automatically update Edge DNS. Both primary and secondary solutions can respond to queries from end users, providing additional availability.
- **Hidden master** – Akamai recommends this deployment option for organizations that wish to continue managing DNS records on an internal DNS solution. The hidden master arrangement allows Edge DNS (as the sole secondary DNS provider, or one of multiple providers) to respond to end-user queries without exposing the internal solution to DDoS attack. Organizations continue managing their DNS records with their primary provider and use zone transfers or Edge DNS APIs to automatically update Edge DNS.
- **Dual primary** – A variant of the hidden master concept. Some cloud service providers no longer embrace the traditional zone transfer functionality and require customers to use their APIs or other user interfaces for zone record changes. Edge DNS can also be leveraged in this method by being configured in primary mode and having the Edge DNS clouds added as authoritative.

Maintaining Availability as Secondary

When deployed as a secondary DNS solution, Edge DNS relies on zone updates from the primary DNS solution to ensure that it responds correctly to end-user queries. Typically, zone files remain valid on a secondary DNS solution for a time-to-live (TTL) period governed by expiry field in the Start of Authority record. A DDoS attack that causes an outage of the primary solution can also cause the secondary solution to stop responding to queries once the outage length exceeds the TTL value. Edge DNS protects against this scenario by (1) holding on to the zone file even after the TTL has expired, and (2) continuing to respond to DNS queries as long as the DNS registry points to Edge DNS. This helps provide additional availability as a secondary DNS solution even if the primary solution is unavailable.

Conclusion

The largest-known DDoS attack now exceeds 1 Tbps in peak bandwidth. At this scale, calculating the total bandwidth available to a cloud-based service no longer provides accurate guidance on its resiliency to such attacks, and even smaller attacks can cause outages at regional levels. Edge DNS employs a multilayered approach to availability to provide 100% availability for customers, combining:

- Massive scale with a global footprint, including name servers and points of presence several times larger than many competing services
- A resilient architecture with numerous segmented IP Anycast clouds to isolate the impact of attacks and prevent collateral damage to other customers as well as the overall platform
- A managed response to DDoS attacks, including the ability to deploy DDoS controls or reassign customer delegations as necessary
- The ability to leverage other Akamai services, including the Akamai CDN and Prolexic DDoS protection, to augment its capacity and withstand DDoS attacks both large and small

Authoritative DNS is a mission-critical service that connects end users around the world with organizations' online presence. Whether deployed as the sole authoritative DNS provider or alongside an existing DNS solution, Edge DNS offers organizations the availability they need to maintain global access to their website and other Internet-facing applications.