WHITE PAPER

Diseño de DNS resiliente y disponible frente a ataques DDoS

Introducción

Edge DNS proporciona a las organizaciones un servicio de DNS autoritativo para conectar a los usuarios finales con sus sitios web y otras aplicaciones. Si bien están muy pendientes del rendimiento, las empresas a menudo pierden de vista la importancia de la disponibilidad y resiliencia del DNS, especialmente frente a los ataques DDoS que pretenden interrumpir el servicio e impedir que los usuarios finales se conecten. Akamai diseñó Edge DNS para garantizar la disponibilidad ante los peores ataques DDoS, con una escala global incomparable, una arquitectura IP Anycast segmentada y numerosos controles de DDoS, incluida la posibilidad de aprovechar otros servicios de Akamai cuando sea necesario. Edge DNS, que se ofrece como un servicio de DNS gestionado, proporciona una combinación óptima de rendimiento y disponibilidad para mantener a las empresas siempre conectadas con sus usuarios finales.

Nota sobre estadísticas

Akamai diseñó originalmente Edge DNS para proporcionar servicios de DNS autoritativos a fin de respaldar sus soluciones de red de distribución de contenido (CDN) globales. A lo largo de los años, Akamai ha aprendido muchas lecciones sobre la mejor forma de escalar y mantener disponible esta gran infraestructura de DNS. Las estadísticas detalladas a la derecha proporcionan una idea general de la magnitud de la plataforma. Sin embargo, las estadísticas por sí solas no pueden proporcionar una panorámica completa de la disponibilidad y la resiliencia, y se deben tener en cuenta junto con la arquitectura de la plataforma, las capacidades de mitigación de ataques DDoS y la capacidad total disponible de Akamai a la hora de proteger la plataforma contra los ataques.

Estadísticas de la plataforma

- Miles de servidores de nombres
- Más de 1000 puntos de presencia
- Más de 140 ciudades
- Más de 40 países

Por motivos de seguridad, Akamai no revela detalles específicos sobre el número de servidores de nombres ni sobre el número, ubicación o tamaño de nuestros puntos de presencia. Esta política protege tanto a Akamai como a nuestros clientes de atacantes que podrían utilizar esa información al planificar ataques.

Arquitectura

Como se puede ver en las estadísticas anteriores, Edge DNS tiene una escala mayor que la mayoría de los servicios de DNS autoritativos que compiten en el mercado actual. Sin embargo, las estadísticas detalladas sobre el número de servidores y puntos de presencia, o la capacidad de red total, son insuficientes para comprender el nivel de disponibilidad y resiliencia de una plataforma global.
A diferencia de otras soluciones de DNS que tradicionalmente se han centrado exclusivamente en el rendimiento, Akamai ha diseñado específicamente Edge DNS para ofrecer disponibilidad y resiliencia frente a los ataques DDoS, además de rendimiento, con redundancias de arquitectura en varios niveles, incluidos servidores de nombres, puntos de presencia, redes e incluso las nubes IP Anycast segmentadas.

IP Anycast

Edge DNS comprende miles de servidores de nombres desplegados en más de 1000 puntos de presencia que emplean un modelo de IP Anycast para responder a las consultas de DNS. IP Anycast dirige las consultas de los usuarios finales al punto más cercano de presencia para su resolución. Junto con un mayor rendimiento, IP Anycast ofrece una serie de ventajas fundamentales en términos de disponibilidad y resiliencia, que es la razón por la que la mayoría de los servicios de DNS autoritativos lo utilizan:

- **Disponibilidad**: IP Anycast permite que los servidores de nombres en diferentes ubicaciones de la red respondan a las consultas dirigidas a una misma dirección IP. Al aprovechar IP Anycast, Edge DNS no solo proporciona a las organizaciones resolución DNS en varios centros de datos, sino que también mejora la disponibilidad mediante la distribución de la carga en todo el mundo. Además, los servidores físicos individuales o puntos de presencia completos pueden desconectarse sin que la capacidad general de resolución de un dominio se vea afectada.

- **Escala**: compuesta por muchos servidores físicos en numerosos puntos de presencia, la infraestructura de Edge DNS proporciona a las organizaciones importantes recursos informáticos en los que siempre pueden confiar al responder a grandes volúmenes de solicitudes de DNS. Edge DNS también tiene acceso a capacidad de red adicional significativa en muchos de sus puntos de presencia, ya que, a menudo, comparte capacidad con otros servicios de Akamai. Esto ofrece a Edge DNS una escala mucho mayor para responder a inundaciones DNS y otras formas de ataques DDoS que un servicio DNS independiente.

- **Distribución**: además de una mayor escala, IP Anycast permite que Edge DNS distribuya el tráfico en varios puntos de presencia y diversas ubicaciones de red. Considerar atentamente las ubicaciones geográficas y las implementaciones de red de estos puntos de presencia puede ayudar a contener el impacto de pequeños ataques en redes o regiones específicas y mantener la disponibilidad de los sistemas del cliente en otras áreas.

Y las ventajas de IP Anycast no se limitan a Akamai. Al permitir que diferentes servidores de nombres resuelvan consultas de DNS de los usuarios finales, IP Anycast mejora la disponibilidad de la resolución de nombres para cualquier servicio DNS. Pero incluso con IP Anycast, la resiliencia sigue limitada por la escala total de la plataforma, y los grandes ataques DDoS pueden seguir saturando una plataforma basada en la nube. Además, sin una arquitectura diversa, incluso los ataques más pequeños tienen el potencial para bloquear servicios DNS en regiones geográficas específicas, lo que los deja inutilizables para muchos usuarios finales y afecta a la disponibilidad de las páginas web a las que los usuarios se conectan.

Nubes de Edge DNS

Para mejorar aún más su resistencia a ataques, Edge DNS segmenta sus servidores de nombres y puntos de presencia en varias nubes IP Anycast. Una nube de Edge DNS consta de servidores de nombres y puntos de presencia dedicados, junto con la capacidad y la conectividad de red asociadas. Las nubes operan de manera independiente y Edge DNS puede ser equivalente a varios proveedores de DNS independientes en términos de disponibilidad, escala y distribución.

Las nubes IP Anycast de Edge DNS representan un conjunto diverso de arquitecturas. Aunque no hay dos nubes idénticas, en general todas cumplen con los dos principios de diseño: rendimiento y disponibilidad:

- **Rendimiento**: la nube de rendimiento puede tener más de 100 puntos de presencia distribuidos alrededor del mundo, y cada uno consta de un conjunto de servidores de nombres. Como se muestra en la Figura 1, una nube de rendimiento despliega pequeños clústeres de servidores de nombres en muchas ubicaciones cercanas a los usuarios finales y proveedores de servicios de Internet (ISP) locales, a fin de proporcionar tiempos de búsqueda más rápidos y un mejor rendimiento bruto. La desventaja es que los pequeños puntos de presencia ofrecen menos resiliencia a los ataques DDoS, por definición, al contar con menos recursos informáticos y menos capacidad de red.
- **Disponibilidad**: Edge DNS mantiene muchas nubes de disponibilidad. Como se muestra en la Figura 1, las nubes de disponibilidad tienen menos puntos de presencia, pero incluyen una o varias regiones delimitadas que pueden incluir cientos de servidores de nombres en un centro de datos centralizado con una gran capacidad de red dedicada y una excelente conectividad a lo largo de múltiples redes. La región delimitada proporciona a la nube de disponibilidad la escala necesaria para responder a grandes picos de solicitudes de DNS y otros tipos de tráfico de red. Las nubes de disponibilidad complementan las regiones delimitadas con una serie de puntos de presencia más pequeños para mantener un nivel aceptable de rendimiento para los usuarios de todo el mundo.

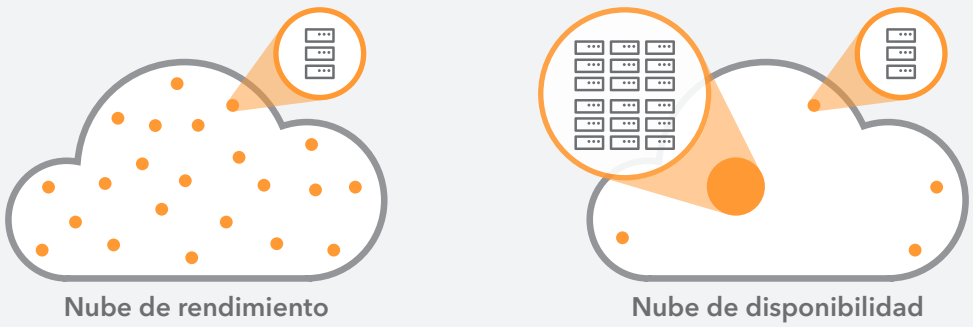

Figura 1: Edge combina varias nubes de DNS con diferentes arquitecturas para ofrecer una combinación óptima de rendimiento, disponibilidad y resiliencia contra ataques DDoS.

Arquitectura segmentada

Edge DNS ofrece fundamentalmente un nivel de disponibilidad diferente, en comparación con otros proveedores de servicios de DNS autoritativos, en una sola nube IP Anycast. Para todos los proveedores, IP Anycast proporciona algunas ventajas en cuestión de disponibilidad, al permitir que el servicio mantenga el tiempo de actividad general durante los ataques más leves que podrían afectar solo a zonas geográficas específicas, en lugar de a toda la plataforma. Sin embargo, incluso las interrupciones localizadas tendrán un impacto en los usuarios finales de las zonas geográficas afectadas, así como en las organizaciones que dependen de dicho servicio para conectar a los usuarios. Además, los ataques DDoS más grandes, con el tráfico generado al atacar sistemas en todo el mundo, tienen el potencial de provocar una interrupción de toda la plataforma.

Gracias al número y diversidad de nubes IP Anycast, Edge DNS puede continuar funcionando incluso con la pérdida de una o varias nubes. Esto proporciona un mayor grado de disponibilidad y resistencia contra ataques DDoS en comparación con una arquitectura de una sola nube. Además, operar en varias nubes IP Anycast ofrece la ventaja de segmentar el tráfico en subsecciones de la plataforma global para mitigar el impacto de los ataques DDoS masivos. Por ejemplo, un ataque contra una sola nube de IP Anycast de Edge DNS se dirigirá a los servidores de nombres físicos y puntos de presencia que componen esa nube específica. La arquitectura segmentada aísla el impacto en otras nubes IP Anycast, lo que permite que Edge DNS mantenga la disponibilidad de la plataforma en todas las zonas geográficas, aunque ciertos clientes o nubes se encuentren bajo un ataque DDoS.

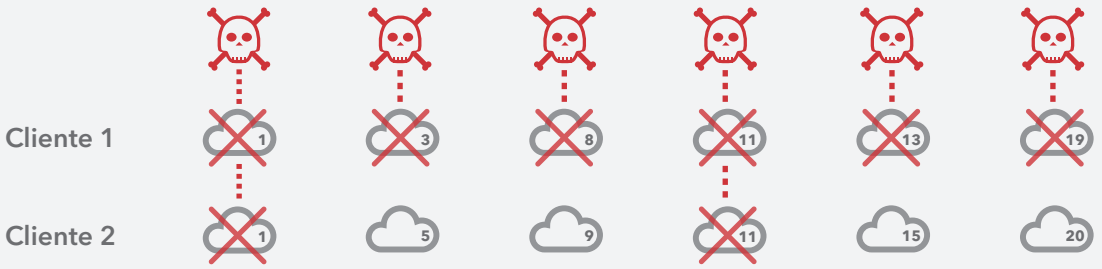

Figura 2: Cada cliente de Edge DNS recibe servidores de nombres en una combinación única de nubes de rendimiento y disponibilidad, lo que minimiza los daños colaterales de un ataque contra otros clientes.

Además de aumentar la resiliencia de la plataforma en general, la arquitectura segmentada de Edge DNS también mitiga el riesgo de daños colaterales para clientes individuales cuando los ataques se dirigen a los servidores de nombres utilizados por otros clientes. Edge DNS asigna a cada cliente varias nubes de Edge DNS, y ofrece una combinación única de nubes de rendimiento y disponibilidad que no se comparten con otros clientes. Como se muestra en la Figura 2, esta distribución minimiza el solapamiento de servidores de nombres y nubes IP Anycast entre dos clientes. También garantiza que cada cliente tenga servidores de nombres que estén disponibles, aunque las nubes IP Anycast asignadas a otro cliente sean el objetivo específico de un ataque DDoS de envergadura.

Gestión de delegaciones del cliente

A menudo, una misma organización es blanco de múltiples ataques DDoS durante un largo periodo de tiempo, y Akamai ha observado extensas campañas de ataque que se han prolongado durante meses. En esta situación, la arquitectura segmentada de Edge DNS ofrece a Akamai una mayor flexibilidad a la hora de minimizar el impacto sobre los clientes que no son blanco del ataque. Como se muestra en la Figura 3, Akamai puede reasignar nubes de un cliente individual y aislar aún más el impacto de un ataque cuando sea necesario.

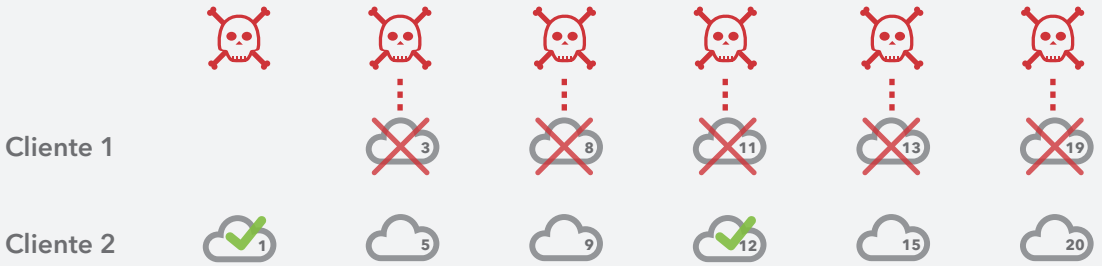

Figura 3: Akamai puede gestionar delegaciones de servidores de nombres para minimizar el impacto de un ataque (en comparación con la Figura 2, arriba), como por ejemplo mover un cliente objetivo fuera de una nube individual y minimizar el solapamiento para clientes que no son el objetivo.

Por ejemplo, Akamai puede:

- **Mover un cliente objetivo fuera una nube específica**: cada cliente de Edge DNS comparte nubes IP Anycast con otros clientes. Como resultado, un ataque que tiene como objetivo todas las nubes de Edge DNS de un cliente en particular puede afectar a la disponibilidad de las nubes que también están asignadas a otros clientes. En circunstancias normales, las resoluciones recursivas cambian automáticamente a nubes con un mejor rendimiento; pero, para campañas sostenidas, Akamai puede reasignar las nubes IP Anycast del cliente objetivo para restaurar la disponibilidad para los clientes que no son el objetivo.

- **Minimizar el solapamiento para clientes que no son el objetivo**: de forma ocasional, varios clientes de Edge DNS pueden compartir un número mayor de lo normal de nubes de Edge DNS. En esta situación, es posible que un ataque masivo contra un único cliente pueda tener un impacto cuantificable en el rendimiento en otros clientes, aunque el servicio general siga disponible. Cuando sea necesario, Akamai puede reasignar las nubes para clientes que no son el objetivo a fin de reducir o eliminar el solapamiento con el cliente objetivo y restaurar el rendimiento para los usuarios finales.

Diversos despliegues de servidores

En cada nube Anycast, Akamai despliega servidores de nombres físicos en diferentes ubicaciones y están diseñados para aumentar la resistencia global de las nubes. Las diversas ubicaciones de nubes de Edge DNS proporcionan otra capa de segmentación del tráfico entre las diferentes redes a fin de maximizar la disponibilidad en diferentes circunstancias. Por ejemplo:

- **En centros de datos con varias redes**: al considerar la resiliencia ante los ataques DDoS, la diversidad de la conectividad de red puede ser tan importante como la propia capacidad. Los ataques DDoS de envergadura pueden saturar los canales de subida ISP y otras redes antes de llegar a un centro de datos, lo que causa una congestión de la red e interrupciones del servicio, aunque el propio centro de datos no se vea afectado. Para mantener la disponibilidad y su capacidad para responder a las consultas de DNS de los usuarios finales durante los ataques, Edge DNS despliega servidores de nombres en grandes centros de datos no solo con altos niveles de capacidad, sino también con conectividad a través de múltiples redes.

- **Aislamiento de ISP**: en muchos casos, Edge DNS despliega clústeres de servidores de nombres directamente en las redes de ISP individuales. Estos servidores de nombres suelen difundir el tráfico de IP Anycast solo dentro de dichas redes y resolver consultas de DNS solo para los usuarios finales de esos ISP. Aunque esta medida limita el número de usuarios finales que puede atender un clúster específico de servidores de nombres, también se preserva la disponibilidad para estos usuarios cuando una nube IP Anycast es el objetivo de un ataque fuera de ese ISP. Un atacante tendría que disponer de sistemas en la red del ISP específico para ver los servidores de nombre e, incluso de esta forma, la capacidad disponible seguiría siendo suficiente para proteger dicha nube.

- **Diversidad de red**: a los clientes se les asigna intencionalmente diversas nubes; algunas con ubicaciones de servidor exclusivas de ISP específicos y algunas con un rango más amplio de máquinas de conexión. Esta arquitectura garantiza que los servidores de nombres recursivos de un cliente determinado siempre puedan conectarse a una nube de Edge DNS disponible.

- **En centros de datos compartidos con otros servicios de Akamai**: al operar diferentes servicios, aparte de DNS autoritativo, Akamai puede desplegar servidores de nombres de Edge DNS en centros de datos que admiten otros servicios. Como se explica con más detalle a continuación, esto permite a Edge DNS contar con una capacidad de red mayor para responder ante ataques DDoS de envergadura; tanto la capacidad de red dedicada como las distribuciones de interconexión pública que tiene Akamai para otros servicios.

Controles de DDoS

Más allá del diseño de su arquitectura, Edge DNS incluye varios controles para ayudar a mitigar el impacto de una categoría de ataques DDoS conocida como inundaciones DNS. Mientras que muchos ataques DDoS utilizan una gran cantidad de tráfico para saturar los enlaces de red, las inundaciones DNS generan grandes volúmenes de solicitudes de DNS legítimas para consumir los recursos informáticos y de memoria en servidores de nombres físicos e impedir que respondan a las consultas de los usuarios finales. Akamai protege la plataforma de Edge DNS contra inundaciones DNS de varias maneras:

- **Escala**: la escala del servicio de DNS autoritativo de Akamai puede ser varias veces superior a la de otras soluciones de DNS de la competencia. Edge DNS utiliza miles de servidores de nombres desplegados en más de 1000 puntos de presencia en todo el mundo. Aunque no es específicamente un control DDoS, IP Anycast reparte el tráfico de ataque entre zonas geográficas y redes, mientras que el número de servidores de nombres físicos proporciona a Edge DNS los recursos informáticos y de memoria necesarios para absorber grandes picos de solicitudes de DNS.

- **Limitación de velocidad**: Edge DNS incluye capacidades de limitación de velocidad y puede disminuir automáticamente las solicitudes de direcciones IP individuales después de que el volumen de solicitudes supere un umbral establecido. La limitación de velocidad evita que grandes picos de solicitudes de DNS consuman recursos informáticos y de memoria en servidores de nombres físicos y puede ser útil a la hora de responder ante ataques que generan un elevado volumen de solicitudes, pero consumen un ancho de banda relativamente bajo. Tenga en cuenta que los clientes no pueden configurar las capacidades de limitación de la velocidad en Edge DNS, sino que se regulan mediante algoritmos exclusivos de la plataforma Edge DNS.

- **Lista blanca de DNS**: dada su posición en Internet, Akamai tiene una visibilidad excepcional del comportamiento de las resoluciones recursivas responsables de aproximadamente el 95 % de las búsquedas de DNS legítimas en Internet. Cuando sea necesario durante una carga pesada, Edge DNS puede emplear un modelo de seguridad positivo y restringir las solicitudes de DNS a una lista de componentes de resolución de DNS conocidos.

Capacidad

Aunque los controles de DDoS pueden ser útiles para mitigar el impacto de inundaciones DNS, otros tipos de ataques DDoS dirigidos a la capa de red requieren la suficiente capacidad de red para absorber el elevado volumen de tráfico. El riesgo de ataques volumétricos ha aumentado drásticamente en los últimos años y los mayores ataques conocidos actualmente superan los 1 Tbps de ancho de banda máximo.

Akamai no revela la capacidad de la plataforma Edge DNS para evitar que los atacantes cuenten con un objetivo cuantificable. Sin embargo, Akamai invierte continuamente en cada aspecto de la escala de la plataforma, e incrementa la infraestructura de Edge DNS para mantener el ritmo de los nuevos clientes y el crecimiento del tráfico en Internet. Como proveedor de servicios en la nube, Akamai puede reasignar rápidamente servidores y desplegar la capacidad de DNS en nuevas regiones. Akamai mantiene una cantidad significativa de capacidad disponible para absorber grandes picos de tráfico, con un tráfico normal en la plataforma Edge DNS que consume menos del 1 % de su capacidad total. Si es necesario, Edge DNS también pueden aprovechar recursos de otras plataformas de Akamai para mitigar los ataques DDoS.

Aprovechamiento de otras plataformas de Akamai

El método tradicional de utilizar la capacidad de red para estimar la capacidad de resistir a un ataque DDoS de gran ancho de banda no funciona con Edge DNS, principalmente porque Edge DNS puede aprovechar recursos de otras plataformas de Akamai. Akamai, que es más que una empresa de DNS, opera muchos servicios además de Edge DNS. De todos los servicios que Akamai opera, el DNS autoritativo es esencial para el funcionamiento de otros servicios, pero sigue siendo pequeño en términos de tráfico global. Esto ofrece varias oportunidades para aumentar la capacidad disponible en Edge DNS cuando es necesario:

- **Tomar prestada la capacidad de la CDN**: en muchos casos, Edge DNS despliega servidores de nombres en los mismos puntos de presencia que los servidores que pertenecen a otros servicios de Akamai y que se ejecutan en la CDN de Akamai. Estos puntos de presencia suelen ser más grandes, ya que están diseñados para respaldar servicios que consumen un ancho de banda mucho mayor. Esto también ofrece a Akamai la flexibilidad operativa necesaria para tomar prestada capacidad de la CDN cuando es necesario. Para ello, se desvían otros servicios a través de otros puntos de presencia de Akamai y la capacidad de red compartida se pone a disposición exclusiva de Edge DNS para que pueda absorber ataques DDoS de envergadura.
- **Desplegar la capacidad de mitigación dedicada**: además de la CDN y del DNS autoritativo, Akamai opera un servicio de protección DDoS independiente con capacidades de mitigación dedicadas. Cuando sea necesario para mitigar ataques DDoS de envergadura, Akamai puede asignar delegaciones de servidores de nombres individuales a través de sus centros de barrido Prolexic para aprovechar las herramientas de mitigación de DDoS y la capacidad dedicada. Esto despliega de manera eficaz las capacidades de mitigación de DDoS de la plataforma Prolexic para Edge DNS, lo que preserva los recursos de Edge DNS a fin de responder a las consultas legítimas de los usuarios finales.

Varios proveedores de DNS

Edge DNS ofrece un servicio de DNS autoritativo con una escala varias veces superior a la de muchos servicios de la competencia, una arquitectura resiliente con numerosas nubes IP Anycast segmentadas y la posibilidad de aprovechar las capacidades adicionales de otros servicios de Akamai para protegerse frente a ataques DDoS. Con estas ventajas, Edge DNS puede proporcionar la disponibilidad y la resiliencia necesarias para operar como proveedor exclusivo de DNS autoritativo para una organización. Sin embargo, algunas organizaciones pueden optar por desplegar Edge DNS junto con su solución existente. Un despliegue multiproveedor permite a las organizaciones mantener sus prácticas de gestión de registros de DNS existentes y, al mismo tiempo, complementar su solución de DNS principal con la disponibilidad y redundancia adicionales de Edge DNS.

Opciones de despliegue

Edge DNS admite diversas opciones para su despliegue en un entorno de varios proveedores:

- **Opción "secundaria tradicional"**: las organizaciones que ya cuentan con un proveedor de DNS pueden desplegar Edge DNS como servicio secundario para complementar su solución de DNS principal. Las organizaciones continuarán gestionando sus registros de DNS con su proveedor primario y usarán transferencias de zona o las API de Edge DNS para actualizar automáticamente Edge DNS. Las soluciones primarias y secundarias pueden responder a las consultas de los usuarios finales, lo que ofrece mayor disponibilidad.

- **Opción "principal oculta"**: Akamai recomienda esta opción de despliegue para las organizaciones que deseen continuar con la gestión de registros de DNS en una solución de DNS interna. Esta opción permite que Edge DNS (como el único proveedor de DNS secundario, o uno de varios proveedores) responda a las consultas del usuario final sin exponer la solución interna a un ataque DDoS. Las organizaciones continuarán gestionando sus registros de DNS con su proveedor primario y usarán transferencias de zona o las API de Edge DNS para actualizar automáticamente Edge DNS.

- **Opción "principal dual"**: es una variante del concepto "principal oculta". Algunos proveedores de servicios en la nube ya no adoptan la funcionalidad de transferencia de zona tradicional y exigen que los clientes utilicen sus API u otras interfaces de usuario para modificar los registros de zona. Edge DNS también se puede aprovechar de esta forma, configurándolo en modo primario y haciendo que las nubes de Edge DNS se agreguen como autoritativas.

Mantenimiento de la disponibilidad como solución secundaria

Cuando se despliega como una solución de DNS secundaria, Edge DNS se basa en las actualizaciones de zona de la solución de DNS primaria para garantizar que responde correctamente a las consultas de los usuarios finales. Normalmente, los archivos de zona siguen siendo válidos en una solución de DNS secundaria para un periodo de vida (TTL) regulado por el campo de caducidad en el registro de inicio de autoridad (SOA). Un ataque DDoS que provoca una interrupción de la solución primaria también puede causar que la solución secundaria deje de responder a las consultas una vez que la duración de la interrupción supere el valor de TTL. Edge DNS protege frente a este escenario; para ello, (1) conserva el archivo de zona aunque se haya superado el valor de TTL, y (2) sigue respondiendo a las consultas de DNS mientras el registro de DNS apunta a Edge DNS. Esto ofrece una disponibilidad adicional como solución de DNS secundaria, aunque la solución primaria no esté disponible.

Conclusión

El ataque DDoS más grande conocido hasta la fecha supera 1 Tbps de ancho de banda pico. A esta escala, calcular el ancho de banda total disponible para un servicio basado en la nube ya no proporciona una orientación precisa sobre su resistencia a esos ataques, e incluso los ataques más pequeños pueden causar interrupciones en los niveles regionales. Edge DNS emplea un enfoque multicapa, en cuanto respecta a la disponibilidad, para proporcionar a los clientes una disponibilidad del 100 %; para ello, combina:

- Escala masiva con una presencia global, incluidos los servidores de nombres y puntos de presencia varias veces más grandes que los de muchos servicios de la competencia.
- Una arquitectura resiliente con numerosas nubes IP Anycast segmentadas para aislar el impacto de los ataques y evitar daños colaterales a otros clientes, así como a la plataforma global.
- Una respuesta gestionada a los ataques DDoS, incluida la capacidad de desplegar controles de DDoS o reasignar las delegaciones del cliente según sea necesario.
- La capacidad de aprovechar otros servicios de Akamai, incluidos la CDN y la protección DDoS de Prolexic, a fin de aumentar su capacidad y resistir los ataques DDoS, tanto grandes como pequeños.

El DNS autoritativo es un servicio fundamental que conecta a los usuarios finales de todo el mundo con organizaciones con presencia online. Si se despliega como único proveedor de DNS autoritativo o junto con una solución de DNS existente, Edge DNS ofrece a las organizaciones la disponibilidad que necesitan para mantener el acceso global a su sitio web y otras aplicaciones orientadas a Internet.

Akamai potencia y protege la vida online. Las empresas más innovadoras de todo el mundo eligen Akamai para proteger y ofrecer sus experiencias digitales, ayudando así a miles de millones de personas a vivir, trabajar y jugar cada día. Gracias a la mayor y más fiable plataforma en el Edge, Akamai acerca las aplicaciones, el código y las experiencias a los usuarios, y mantiene alejadas las amenazas. Obtenga más información sobre los productos y servicios de seguridad, distribución de contenido y Edge Computing de Akamai en www.akamai.com y blogs.akamai.com, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en marzo de 2020.