WHITE PAPER

Progettazione di un'infrastruttura DNS in grado di garantire disponibilità e resilienza contro gli attacchi DDoS

Introduzione

Edge DNS fornisce alle organizzazioni un servizio DNS autoritativo per connettere gli utenti finali ai loro siti web e ad altre applicazioni. Le organizzazioni, spesso, concentrano la propria attenzione sulle performance trascurando l'importanza di un DNS sempre disponibile e resiliente, in grado di contrastare gli attacchi DDoS che mirano a interrompere il servizio e impedire agli utenti finali di connettersi. Akamai ha progettato Edge DNS per restare disponibile anche durante i più imponenti attacchi DDoS, con una scalabilità su scala globale impareggiabile, un'architettura IP Anycast segmentata e molteplici controlli DDoS, inclusa la possibilità di sfruttare altri servizi Akamai quando necessario. Offerto come servizio DNS gestito, Edge DNS offre un'ottima combinazione di performance e disponibilità per connettere sempre le organizzazioni ai loro utenti finali.

Nota sulle statistiche

Akamai aveva creato originariamente Edge DNS per fornire i servizi DNS autoritativi a supporto delle sue soluzioni CDN (rete per la distribuzione dei contenuti) globali. Nel corso degli anni, Akamai ha imparato molte lezioni su come scalare al meglio e rendere disponibile un'infrastruttura DNS così ampia. Le statistiche generali a destra offrono un quadro complessivo della scalabilità della piattaforma. Tuttavia, le statistiche da sole non possono offrire una guida significativa sulla disponibilità e la resilienza, e devono essere considerate insieme all'architettura della piattaforma, alle funzionalità di mitigazione di attacchi DDoS specifici, e alla capacità complessiva disponibile per Akamai quando deve proteggere la piattaforma dagli attacchi.

Statistiche della piattaforma

- Migliaia di server dei nomi
- Oltre 1.000 punti di presenza
- Più di 140 città
- Più di 40 paesi

Tenete presente che Akamai non divulga dettagli specifici sul numero di server dei nomi o numeri, posizioni o dimensioni dei punti di presenza per ragioni di sicurezza. Questa politica protegge Akamai e i suoi clienti da malintenzionati che potrebbero tentare di usare queste informazioni per la pianificazione degli attacchi.

Architettura

Come potete vedere dalla statistica sopra, Edge DNS vanta una scalabilità superiore a quella della maggior parte dei servizi DNS autoritativi della concorrenza disponibili nel mercato di oggi. Tuttavia, le statistiche generali sul numero di server e punti di presenza, oppure la quantità della capacità di rete totale, sono insufficienti per comprendere il livello di disponibilità e resilienza per una piattaforma globale. A differenza di altre soluzioni DNS incentrate tradizionalmente sulle performance, Akamai ha progettato specificamente Edge DNS per la disponibilità e la resilienza contro gli attacchi DDoS, in aggiunta alle performance, con ridondanze delle architetture a livelli multipli, inclusi server dei nomi, punti di presenza, reti e anche i cloud IP Anycast segmentati.

IP Anycast

Edge DNS comprende migliaia di server dei nomi implementati in oltre 1.000 punti di presenza, che impiegano il modello IP Anycast per rispondere alle query DNS. IP Anycast indirizza le query degli utenti finali al più vicino punto di presenza affinché vengano risolte. Oltre a performance più rapide, IP Anycast offre diversi vantaggi fondamentali per la disponibilità e la resilienza, ecco perché viene utilizzato dalla maggior parte dei servizi DNS autoritativi:

- **Disponibilità**: IP Anycast consente ai server dei nomi in posizioni di rete diverse di rispondere alle query inviate a un singolo indirizzo IP. Sfruttando IP Anycast, Edge DNS non solo fornisce alle organizzazioni una risoluzione DNS in molteplici data center, ma migliora anche la disponibilità distribuendo il carico globalmente. Inoltre, singoli server fisici o interi punti di presenza possono andare offline senza influire sulla capacità complessiva di risoluzione di un dominio.

- **Scalabilità**: includendo molti server fisici in numerosi punti di presenza, l'infrastruttura Edge DNS fornisce alle organizzazioni significative risorse di elaborazione sulle quali possono fare affidamento costantemente per rispondere ai grandi volumi di richieste DNS. Edge DNS ha inoltre accesso a significative capacità di rete aggiuntive in molti dei suoi punti di presenza, in quanto condivide spesso la capacità con altri servizi Akamai. Ciò consente a Edge DNS una maggiore scalabilità per rispondere ai flood DNS e ad altre forme di attacchi DDoS rispetto a un servizio DNS autonomo.

- **Distribuzione**: oltre a consentire una scalabilità maggiore, IP Anycast permette a Edge DNS di distribuire il traffico su più punti di presenza e posizioni di rete diverse. La considerazione ponderata delle posizioni geografiche e delle distribuzioni di rete per questi punti di presenza può aiutare a contenere l'impatto degli attacchi più piccoli a geografie o reti specifiche, e a preservare la disponibilità per i sistemi client in altre aree.

Akamai non è l'unica a servirsi di IP Anycast. Consentendo a più server dei nomi di risolvere le query DNS degli utenti finali, IP Anycast migliora la disponibilità della risoluzione dei nomi per qualsiasi servizio DNS. Ma persino con IP Anycast, la resilienza resta limitata dalla scalabilità totale della piattaforma e attacchi DDoS di grandi dimensioni possono comunque sopraffare una piattaforma basata su cloud. Per di più, senza un'architettura diversificata, persino gli attacchi più piccoli possono potenzialmente arrestare i servizi DNS in aree geografiche specifiche, rendendoli non disponibili per un gran numero di utenti finali e influendo sulla disponibilità dei siti web ai quali quegli stessi utenti si collegano.

Cloud Edge DNS

Per migliorare ulteriormente la sua resilienza contro gli attacchi, Edge DNS segmenta i suoi server dei nomi e i punti di presenza in più cloud IP Anycast. Un cloud Edge DNS è costituito da server dei nomi e punti di presenza insieme alle capacità e connettività di rete a questi associate. Ogni cloud opera in modo indipendente dall'altro, e Edge DNS può essere equivalente a più provider DNS autonomi in termini di disponibilità, scalabilità, e distribuzione.

I cloud IP Anycast di Edge DNS rappresentano un diversificato set di architetture. Anche se due cloud non sono mai identici, si allineano ampiamente a due principi di progettazione: performance e disponibilità:

- **Performance**: un cloud delle performance può avere più di 100 punti di presenza distribuiti in tutto il mondo, ognuno dei quali comprende un insieme di server dei nomi. Come mostrato nella Figura 1, un cloud delle performance implementa piccoli cluster di server dei nomi in più posizioni vicine agli utenti finali e ISP (Internet Service Provider) locali, al fine di fornire tempi di ricerca più rapidi e migliori performance semplici. Il compromesso sta nel fatto che, per definizione, i piccoli punti di presenza offrono meno resilienza rispetto agli attacchi DDoS, avendo a disposizione meno risorse di elaborazione e meno capacità di rete.
- **Disponibilità**: Edge DNS gestisce molti cloud della disponibilità. Come mostrato nella Figura 1, i cloud della disponibilità hanno meno punti di presenza, ma dispongono di una o più aree di ancoraggio che possono includere centinaia di server dei nomi in un data center centralizzato, con un'ampia disponibilità di capacità di rete dedicata e connettività attraverso più reti. L'area di ancoraggio offre a un cloud della disponibilità la scalabilità adatta a rispondere a grandi picchi di richieste DNS e a un traffico di rete di altro tipo. I cloud della disponibilità ampliano le aree di ancoraggio con un numero ridotto di punti di presenza più piccoli, per gestire un livello accettabile di performance per gli utenti di tutto il mondo.

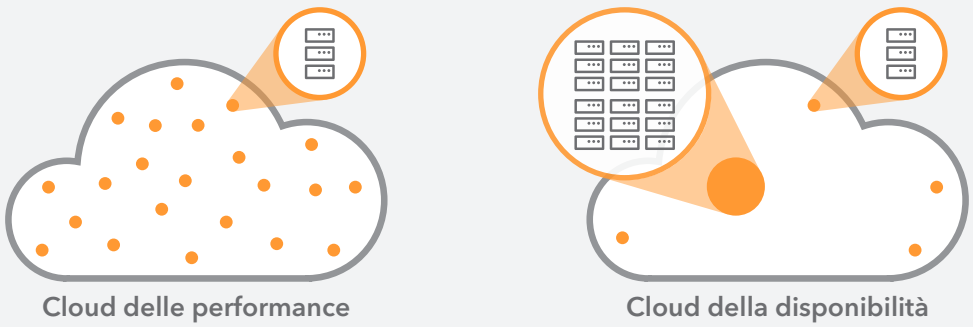

Figura 1: Edge DNS unisce più cloud DNS a varie architetture per offrire una combinazione ottimale di performance, disponibilità e resilienza contro gli attacchi DDoS.

Architettura segmentata

Edge DNS offre un livello sostanzialmente diverso di disponibilità rispetto ad altri provider che utilizzano servizi DNS autoritativi su un solo cloud IP Anycast. Per tutti i provider, IP Anycast offre alcuni vantaggi in fatto di disponibilità, consentendo ai servizi di mantenere tempi di attività complessivi in caso di piccoli attacchi che potrebbero colpire aree geografiche specifiche piuttosto che l'intera piattaforma. Tuttavia, persino le interruzioni circoscritte interesseranno gli utenti finali nelle aree colpite, come anche le organizzazioni che si affidano a un dato servizio per collegarsi a tali utenti. Inoltre, i grandi attacchi DDoS, con il traffico generato dai sistemi di attacco nel mondo, possono potenzialmente causare un'interruzione dell'intera piattaforma.

Con cloud IP Anycast vari e diversificati, Edge DNS può continuare a funzionare persino in caso di perdita di uno o più cloud. Ciò offre un maggiore livello di disponibilità e resilienza contro gli attacchi DDoS rispetto a un'architettura cloud singola. Inoltre, l'utilizzo di più cloud IP Anycast offre il vantaggio

di poter segmentare il traffico in sottosezioni dell'intera piattaforma, al fine di mitigare anche l'impatto degli attacchi DDoS più importanti. Ad esempio, un attacco contro un cloud IP Anycast con Edge DNS singolo sarà indirizzato contro i server dei nomi fisici e i punti di presenza fisici che costituiscono quel dato cloud. L'architettura segmentata isola l'impatto da altri cloud IP Anycast, consentendo a Edge DNS di mantenere la disponibilità della piattaforma in tutte le aree, anche nel caso in cui singoli cloud o clienti fossero sotto attacco DDoS.

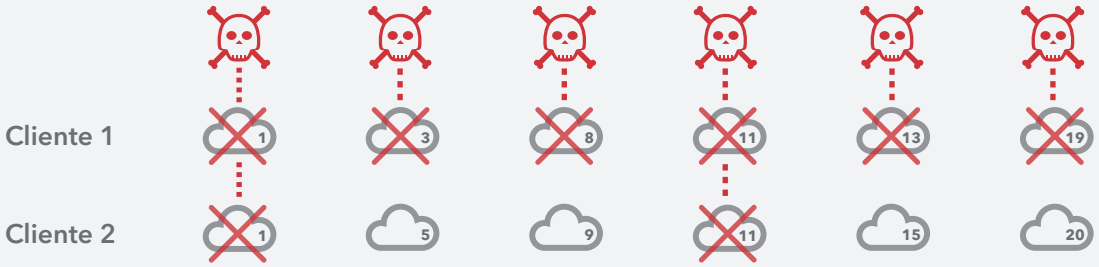

Figura 2: tutti i clienti di Edge DNS ricevono server dei nomi su una combinazione unica di cloud di performance e della disponibilità, riducendo al minimo i danni collaterali derivanti da un attacco sferrato contro altri clienti.

Oltre ad aumentare la resilienza complessiva della piattaforma, l'architettura segmentata di Edge DNS mitiga anche il rischio di danni collaterali per i singoli clienti nel caso in cui i server dei nomi utilizzati da altri clienti vengano attaccati. Edge DNS assegna a ogni cliente più cloud Edge DNS, in una combinazione unica tra cloud di performance e della disponibilità, mai vista da nessun altro cliente. Come mostrato nella Figura 2, questa distribuzione riduce al minimo la sovrapposizione nei server dei nomi e nei cloud IP Anycast tra due dati clienti. Garantisce, inoltre, che ogni cliente avrà a disposizione server dei nomi anche quando i cloud IP Anycast assegnati a un altro cliente sono specificamente colpiti da un attacco DDoS di grandi dimensioni.

Gestione delle deleghe dei clienti

Diversi attacchi DDoS contro una sola organizzazione spesso si verificano per periodi più lunghi e Akamai ha visto durare per mesi e mesi campagne di attacchi ampie e continue. In una situazione del genere, l'architettura segmentata di Edge DNS offre ad Akamai una maggiore flessibilità nel ridurre ulteriormente l'impatto sui clienti non colpiti dall'attacco. Come mostrato nella Figura 3, Akamai può riassegnare i cloud di un singolo cliente e isolare ulteriormente l'impatto di un attacco, se necessario.

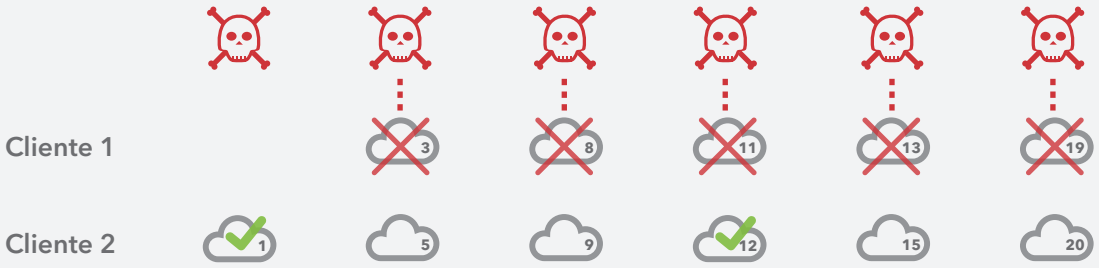

Figura 3: Akamai può gestire deleghe di server dei nomi per ridurre ulteriormente l'impatto di un attacco (rispetto alla Figura 2, sopra), ad esempio spostando un cliente colpito da un determinato cloud e riducendo al minimo la sovrapposizione con i clienti non colpiti.

Ad esempio, Akamai può:

- **Trasferire un cliente colpito su un cloud specifico**: ogni cliente di Edge DNS condivide cloud IP Anycast con altri clienti. Di conseguenza, un attacco mirato a tutti i cloud Edge DNS di un cliente può influenzare anche la disponibilità dei cloud assegnati ad altri clienti. In circostanze normali, i risolutori ricorsivi passano automaticamente a cloud più performanti, ma per le campagne prolungate Akamai può riassegnare i cloud IP Anycast del cliente colpito, al fine di ripristinare la disponibilità per i clienti non colpiti.
- **Ridurre al minimo le sovrapposizioni per i clienti non colpiti**: a volte, i clienti di Edge DNS possono condividere un numero più alto del normale di cloud Edge DNS. In questo caso, è possibile che un attacco imponente contro un solo cliente possa avere un impatto misurabile sulle performance di altri clienti, nonostante il servizio complessivo resti comunque disponibile. Se necessario, Akamai può riassegnare i cloud per i clienti non colpiti, al fine di ridurre o eliminare la sovrapposizione con il cliente colpito e ripristinare le performance per i propri utenti finali.

Implementazioni diversificate dei server

All'interno di ogni cloud Anycast, Akamai implementa server dei nomi fisici in vari punti, al fine di aumentare la resilienza complessiva del cloud stesso. Posizioni di cloud Edge DNS diverse forniscono un ulteriore livello di segmentazione del traffico su più reti, per massimizzare la disponibilità in varie circostanze. Per fare qualche esempio:

- **Nei data center con più reti**: nel valutare la resilienza contro gli attacchi DDoS, la diversità nella connettività di rete può essere importante quanto la sua stessa capacità. Attacchi DDoS di grandi dimensioni possono sopraffare gli ISP a monte e altre reti prima di raggiungere un data center, causando una congestione della rete e interruzioni dei servizi anche nel caso in cui il data center stesso non venga colpito. Per mantenere la sua disponibilità e capacità di rispondere alle query DNS degli utenti finali durante gli attacchi, Edge DNS implementa server dei nomi in grandi data center dotati non solo di grandi capacità, ma anche di connettività attraverso più reti.
- **Isolamento degli ISP**: in molti casi, Edge DNS implementa cluster di server dei nomi direttamente nelle reti dei singoli ISP. Questi server dei nomi spesso trasmettono il proprio traffico IP Anycast solo all'interno di quelle reti e risolvono le query DNS degli utenti finali di quegli ISP. Se da un lato questa decisione limita il numero di utenti finali che un cluster specifico di server dei nomi può gestire, dall'altro mantiene la disponibilità per quegli stessi utenti quando un cloud IP Anycast viene preso di mira da un attacco al di fuori dell'ISP. L'autore di un attacco dovrebbe avere dei sistemi sulla rete di quel dato ISP specifico per poter vedere quei server dei nomi e, persino in quel caso, la capacità disponibile spesso basta a proteggere quel cloud.
- **Diversità di rete**: i clienti vengono assegnati intenzionalmente a diversi cloud, alcuni con posizioni di server uniche per ISP specifici e altri con una portata più ampia di macchine connesse. Quest'architettura garantisce che i server dei nomi ricorsivi di un dato cliente siano sempre in grado di connettersi a un cloud Edge DNS disponibile.

- **Nei data center condivisi con altri servizi Akamai**: utilizzando molti servizi diversi oltre al DNS autoritativo, Akamai può implementare server dei nomi Edge DNS nei data center che supportano più servizi. Come descritto più nel dettaglio, ciò consente a Edge DNS di accedere a una più ampia capacità di rete quando deve rispondere ad attacchi DDoS di grandi dimensioni: una capacità di rete dedicata e disposizioni di peering pubblico che Akamai ha già implementato per altri servizi.

Controlli DDoS

Oltre alla sua progettazione di architettura, Edge DNS comprende vari controlli per favorire la mitigazione dell'impatto di una categoria di attacchi DDoS nota come flood DNS. Se da un lato molti attacchi DDoS utilizzano una grande quantità di traffico per sopraffare i collegamenti di rete, i flood DNS generano grandi volumi di richieste DNS legittime al fine di consumare le risorse di elaborazione e di memoria di cui dispongono i server dei nomi fisici, per impedire loro di rispondere alle query degli utenti finali reali. Akamai protegge la piattaforma Edge DNS dai flood DNS in molti modi:

- **Scalabilità**: la scalabilità del servizio DNS autoritativo di Akamai può essere diverse volte maggiore rispetto a quella delle soluzioni DNS concorrenti. Edge DNS utilizza migliaia di server dei nomi distribuiti in più di 1000 punti di presenza in tutto il mondo. Anche se non è prettamente un controllo DDoS, IP Anycast distribuisce il traffico degli attacchi su aree e reti, mentre il numero dei server dei nomi fisici offre a Edge DNS risorse di elaborazione e memoria sufficienti ad assorbire i grandi picchi di richieste DNS.

- **Limitazione della velocità**: Edge DNS comprende funzionalità di limitazione della velocità e può eliminare automaticamente le richieste di singoli indirizzi IP quando il volume delle richieste supera una certa soglia. La limitazione della velocità impedisce ai grandi picchi di richieste DNS di consumare le risorse di elaborazione e memoria sui server dei nomi fisici e può essere utile nella risposta agli attacchi che generano un ampio volume di richieste, ma consumano una larghezza di banda relativamente bassa. È da notare che le funzioni di limitazione della velocità su Edge DNS non possono essere configurate dai clienti, ma vengono utilizzate da algoritmi univoci per la piattaforma Edge DNS.

- **Whitelist DNS**: grazie alla sua posizione su Internet, Akamai ha una visibilità unica sul comportamento dei risolutori ricorsivi responsabili di circa il 95% delle ricerche del DNS legittime su Internet. Se necessario, nei periodi di maggior carico, Edge DNS può implementare un modello di sicurezza positivo e limitare le richieste DNS a un elenco di risolutori DNS noti.

Per quanto riguarda la capacità

Se i controlli DDoS possono essere utili a mitigare l'impatto dei flood DNS, altri tipi di attacchi DDoS a livello di rete richiedono la disponibilità di una capacità di rete sufficiente ad assorbire l'elevato volume di traffico. Il rischio di attacchi volumetrici è aumentato vertiginosamente negli ultimi anni e i più vasti attacchi conosciuti ora superano di gran lunga 1 Tbps nei picchi di larghezza di banda.

Akamai non divulga la capacità della piattaforma Edge DNS, onde evitare di fornire agli autori degli attacchi una preda tangibile. Tuttavia, Akamai investe con costanza in ogni aspetto della scalabilità della piattaforma, ampliando l'infrastruttura Edge DNS, per tenerla al passo con i nuovi clienti e la crescita del traffico su Internet. In qualità di provider di servizi cloud, Akamai può riutilizzare rapidamente i server e implementare capacità DNS in nuove aree. Akamai gestisce una capacità notevole per assorbire il traffico nei momenti di grande picco, mentre il traffico normale sulla piattaforma Edge DNS consuma meno dell'1% della sua capacità complessiva. Se necessario, Edge DNS può anche servirsi di risorse provenienti da altre piattaforme Akamai per mitigare gli attacchi DDoS.

Utilizzo di altre piattaforme Akamai

Il metodo tradizionale dell'utilizzo della capacità di rete per valutare la capacità di resistenza a un attacco DDoS a larghezza di banda elevata non funziona con Edge DNS, principalmente perché esso può servirsi di risorse provenienti da altre piattaforme Akamai. Akamai, che è molto più di una semplice azienda, gestisce molti servizi oltre a Edge DNS. Di tutti i servizi gestiti da Akamai, il DNS autoritativo è fondamentale per l'utilizzo di altri servizi, ma consuma una piccola quantità del traffico complessivo. Ciò offre diverse opportunità di aumentare la capacità disponibile per Edge DNS, qualora sia necessario:

- **Capacità presa in prestito dalla CDN**: in molti casi, Edge DNS implementa server dei nomi all'interno degli stessi punti di presenza dei server che appartengono ad altri servizi di Akamai in esecuzione sulla CDN di Akamai. Questi punti di presenza sono spesso molto più grandi, poiché progettati per supportare servizi che consumano una larghezza di banda molto più ampia. Ciò conferisce inoltre ad Akamai la flessibilità necessaria a prendere in prestito la capacità della CDN se è necessario, direzionando altri servizi attraverso altri punti di presenza di Akamai e rendendo disponibile la capacità di rete condivisa solo a Edge DNS, perché possa assorbire gli attacchi DDoS di grandi dimensioni.
- **Implementazione di una capacità di mitigazione dedicata**: oltre al DNS autoritativo e alla CDN, Akamai gestisce un servizio di protezione contro gli attacchi DDoS a parte, con capacità e funzionalità di mitigazione dedicate. Quando deve mitigare attacchi DDoS di grandi dimensioni, Akamai può assegnare deleghe di server dei nomi individuali grazie ai suoi scrubbing center Prolexic, per sfruttare quella capacità e quegli strumenti di mitigazione degli attacchi DDoS dedicati. Ciò consente di implementare in modo efficace le funzionalità di mitigazione degli attacchi DDoS della piattaforma Prolexic su Edge DNS, conservando le risorse di Edge DNS per la risposta alle query legittime degli utenti finali.

Più fornitori DNS

Edge DNS offre un servizio DNS autoritativo con una scalabilità diverse volte maggiore rispetto ai servizi della concorrenza, un'architettura resiliente con vari cloud IP Anycast segmentati, nonché la possibilità di sfruttare le capacità e funzionalità aggiuntive di altri servizi di Akamai per proteggersi da attacchi DDoS. Con questi vantaggi, Edge DNS può fornire la disponibilità e la resilienza necessarie a fungere da provider DNS autoritativo unico per un'organizzazione. Tuttavia, alcune organizzazioni potrebbero decidere di implementare Edge DNS insieme alla loro soluzione esistente. Un'implementazione multi-vendor consente alle organizzazioni di mantenere le proprie procedure di gestione dei record DNS, integrando al tempo stesso la propria soluzione DNS primaria con la disponibilità e la ridondanza aggiuntive di Edge DNS.

Opzioni di distribuzione

Edge DNS supporta diverse opzioni di distribuzione per Edge DNS in un ambiente multi-vendor:

- **Servizio secondario tradizionale**: le organizzazioni dotate di un altro provider DNS possono distribuire Edge DNS come servizio secondario per ampliare la propria soluzione DNS primaria. Le organizzazioni continuano a gestire i propri record DNS con il provider primario e utilizzano trasferimenti di zone o API Edge DNS per aggiornare automaticamente Edge DNS. Sia le soluzioni primarie che quelle secondarie possono rispondere alle query degli utenti finali, per una maggiore disponibilità.

- **Master nascosto**: Akamai consiglia questa opzione di distribuzione alle organizzazioni che desiderano continuare a gestire i record DNS su una soluzione DNS interna. L'opzione Master nascosto consente a Edge DNS (in quanto unico provider DNS secondario o uno di più provider) di rispondere alle query degli utenti finali senza esporre la soluzione interna agli attacchi DDoS. Le organizzazioni continuano a gestire i propri record DNS con il provider primario e utilizzano trasferimenti di zone o API Edge DNS per aggiornare automaticamente Edge DNS.

- **Primario doppio**: una variante del concetto di Master nascosto. Alcuni provider di servizi cloud non adottano più la funzionalità tradizionale di trasferimento delle zone e hanno bisogno che i propri clienti utilizzino le proprie API o altre interfacce utente per modificare i record delle zone. Edge DNS può essere utilizzato anche in questo metodo, configurandolo come primario e aggiungendo i cloud Edge DNS come autoritativi.

Mantenimento della disponibilità come soluzione secondaria

Quando viene distribuito come soluzione DNS secondaria, Edge DNS si basa sugli aggiornamenti delle zone della soluzione DNS primaria per garantire una risposta corretta alle query degli utenti finali. In genere, i file delle zone restano validi su una soluzione DNS secondaria per un periodo TTL regolato dal campo Scadenza nel record Origine di autorità. Un attacco DDoS che causa un'interruzione della soluzione primaria può portare anche quella secondaria a non rispondere alle query se la lunghezza del periodo di interruzione supera il valore TTL. Edge DNS protegge da queste situazioni (1) conservando il file della zona anche dopo la scadenza del TTL e (2) continuando a rispondere alle query DNS fino a quando il registro DNS punta a Edge DNS. La soluzione DNS secondaria offre un'ulteriore disponibilità, anche quando la soluzione primaria non è disponibile.

Conclusione

Il più vasto attacco DDoS conosciuto ora supera 1 Tbps nei picchi di larghezza di banda. A una tale velocità, il calcolo della larghezza di banda complessiva di un servizio basato sul cloud non fornisce più una traccia adeguata in merito alla sua resilienza a tali attacchi e persino gli attacchi più piccoli possono causare interruzioni a livello di zone. Edge DNS utilizza un approccio multilivello alla disponibilità per offrire una disponibilità del 100% ai clienti, combinando:

- Enorme portata e presenza globale, con server dei nomi e punti di presenza diverse volte più grandi rispetto a quelli di molti servizi concorrenti.
- Un'architettura resiliente con numerosi cloud IP Anycast segmentati per isolare l'impatto degli attacchi e prevenire danni collaterali ad altri clienti e alla piattaforma intera.
- Una risposta gestita per gli attacchi DDoS, che comprende la possibilità di distribuire controlli DDoS o riassegnare deleghe dei clienti, se necessario.
- La possibilità di sfruttare altri servizi di Akamai, come la CDN di Akamai e la protezione contro gli attacchi DDoS Prolexic per aumentare la capacità e la resistenza agli attacchi DDoS di piccole e grandi dimensioni.

Il DNS autoritativo è un servizio mission-critical che collega gli utenti finali di tutto il mondo alla presenza online delle organizzazioni. Se distribuito come unico provider DNS autoritativo o utilizzato insieme a una soluzione DNS esistente, Edge DNS offre alle organizzazioni la disponibilità necessaria a mantenere un accesso globale al proprio sito web e ad altre applicazioni connesse a Internet.

Akamai promuove e protegge la vita online. Le aziende più innovative al mondo scelgono Akamai per proteggere e offrire le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Con la più ampia e affidabile piattaforma edge al mondo, Akamai è in grado di tenere vicine agli utenti experience, codici e app e lontane le minacce. Per scoprire ulteriori informazioni sulla sicurezza, sulla delivery dei contenuti e sui servizi e prodotti per l'Edge Computing di Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 03/20.